An Examination of E-Banking Fraud Prevention and Detection in Nigerian Banks

BY

Oluwalami Matthew Fadayo

Thesis submitted to the Doctoral College, De Montfort University, in partial fulfilment of the requirements for the Degree of Doctor of Philosophy

Faculty of Business & Law, Department of Accounting & Finance

November, 2018

ABSTRACT

E-banking offers a number of advantages to financial institutions, including convenience in terms of time and money. However, criminal activities in the information age have changed the way banking operations are performed. This has made e-banking an area of interest. The growth of cybercrime – particularly hacking, identity theft, phishing, Trojans, service denial attacks and account takeover– has created several challenges for financial institutions, especially regarding how they protect their assets and prevent their customers from becoming victims of cyber fraud. These criminal activities have remained prevalent due to certain features of cyber, such as the borderless nature of the internet and the continuous growth of the computer networks. Following these identified challenges for financial institutions, this study examines e-banking fraud prevention and detection in the Nigerian banking sector; particularly the current nature, impacts, contributing factors, and prevention and detection mechanisms of e-banking fraud in Nigerian banking institutions.

This study adopts mixed research methods with the aid of descriptive and inferential analysis, which comprised exploratory factor analysis (EFA) and confirmatory factor analysis (CFA) for the quantitative data analysis, whilst thematic analysis was used for the qualitative data analysis. The theoretical framework was informed by Routine Activity Theory (RAT) and Fraud Management Lifecycle Theory (FMLT).

The findings show that the factors contributing to the increase in e-banking fraud in Nigeria include ineffective banking operations, internal control issues, lack of customer awareness and bank staff training and education, inadequate infrastructure, presence of sophisticated technological tools in the hands of fraudsters, negligence of banks' customers concerning their e-banking account devices, lack of compliance with the banking rules and regulations, and ineffective legal procedure and law enforcement. In addition, the enforcement of rules and regulations in relation to the prosecution of financial fraudsters has been passive in Nigeria. Moreover, the findings also show that the activities of each stage of fraud management lifecycle theory are interdependent and have a collective and considerable influence on combating e-banking fraud. The results of the findings confirm that routine activity theory is a real-world theoretical framework while applied to e-banking fraud. Also, from the analysis of the findings, this research offers a new model for e-banking fraud prevention and detection within the Nigerian banking sector. This new model confirms that to have perfect prevention and detection of e-banking fraud there must be presence of technological mechanisms, fraud monitoring, effective internal controls, customer complaints, whistle-blowing, surveillance mechanisms, staff-customer awareness and education, legal and judicial controls, institutional synergy mechanisms of in the banking systems. Finally, the findings from the analyses of this study have some significant implications; not only for academic researchers or scholars and accounting practitioners, but also for policymakers in the financial institutions and anti-fraud agencies in both the private and public sectors.

DEDICATION

This Thesis is dedicated to God Almighty, and to the memory of both my parents through whom I came into this world. My father, late Pa Fatoki, Fadayo Elijah and my late mother, Ruth Oyebimpe Fadayo. They have laboured tirelessly for my education; they did not only nurture and raise me, but also overstretched themselves dearly over the years for my intellectual and educational development.

ACKNOWLEDGEMENTS

I must thank God Almighty for making this PhD programme a success. The work remains a child of my brain only through His enablement.

My orientation was changed by the supervisory team of this study, Dr. Kemi Yekini (Associate Professor), Dr. Paschal Ohalehi and Prof. Emmanuel Adegbite who kept reminding me of the need to give this study all it deserves. They have contributed immeasurably to the achievement of this PhD programme. They are worthy of praise and emulation. I would also acknowledge my thesis examiners Dr. Ama Ayo and Dr. Godwin Okafor, who gave very constructive, productive and positive remarks. I have no iota of regret knowing them. I am most indebted to them. Likewise, I have benefited immensely from the provocative interactions I have had academically with my internal and independent assessors of formal and annual reviews of my thesis, Dr. Neil Lancastle and Fred Mear (Associate Professor) respectively; their guidance and supports at review phases are well appreciated. I am very grateful.

My profound gratitude goes to the all staff of Doctoral College De Montfort University. They are worthy leaders, staff and administrators. I honestly appreciate their words of encouragement, their prompt responses to mails, their moral supports are as quantifiable as their presence and constructive criticism with useful suggestions. I am ever indebted to you all.

I am sincerely grateful to my beautiful and pleasant family, firstly to my lovely wife Mrs. Juliet Nkechi Fadayo. Without her patience, endless support and encouragement, the rigorous process of this study would have been insurmountable. I cannot thank her enough for her understanding, unflinching support and moral backing. She is such a wonderful wife. And to my most precious children, Elijah Wonderful, Elisha Marvellous and Ezekiel Excellent, they were most disregarded during the period of this PhD programme. My nonappearances at home were obviously felt by them. During the period, I might have ignored them and abandoned them to their mother, but I pledge to commit whatever resources necessary to make it up to them. Surely, from now on, they will have my devotion. I sincerely appreciate their patience, understanding and love. I say thanks.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

APPENDICES

TABLE OF ACRONYMS AND ABBREVIATIONS

ACCS	Australian Computer Crime and Security
ACFE	Association of Certified Fraud Examiners
ACFT	Australasian Consumer Fraud Taskforce
AGFI	Adjusted Goodness-of-Fit Index
AIC	Akaike Information Criterion
AICPA	American Institute of Certified Public Accountants
ASSOCHAM	Associated Chambers of Commerce and Industry of India
ATM	Automated Teller Machine
BLAST- SSAHA	Basic Local Alignment Search Tool and Sequence Search and Alignment by Hashing Algorithm
BVN	Bank Verification Number
CA	Content Analysis
CBN	Central Bank of Nigeria
CBs	Commercial Banks
CCTV	Closed Circuit Television
CERTs	Computer Emergency Response Teams
CFA	Confirmatory Factor Analysis
CFI	Comparative Fit Index
CIMA	Chartered Institute of Management Accountants
COER	Cross-Over Error Rate
CSR	Corporate Social Responsibility

CSC	Card Security Code
DFBs	Development Finance Banks
DMBs	Deposit Money Banks
DS	Deviation Score
EFA	Exploratory Factor Analysis
ENISA	European Network and Information Security Agency
FACTA	Fair and Accurate Credits Transactions Acts
FCT	Federal Capital Territory
FDT	Fraud Diamond Theory
FFA UK	Financial Fraud Action United Kingdom
FHD	Fraud History Database
FMLT	Fraud Management Lifecycle Theory
FRIS	Fraud Risk Assessments and Investigations System
FST	Fraud Scale Theory
GFI	Goodness-of-Fit Index
GLS	Generalized Least Squares
HMM.	Hidden Markov Model
IDS	Intrusion Detection System
IFI	Incremental Fit Index
IIA	Institute of Internal Auditors
KMO	Kaiser-Meyer-Olkin
MBs	Merchant Banks

MEM	Modern e-Fraud Mode
MF	Model Fit
MFBs	Micro-Finance Banks
MI	Modification Indices
ML	Maximum Likelihood
NDIC	Nigeria Deposit Insurance Corporation
NFI	Normed Fit Index
NIBs	Non-Interest Banks
NIBSS	Nigeria Inter-Bank Settlement System
NIDC	Nigeria Deposit Insurance Corporation
OTPs	One-Time Password
PFI	Parsimonious Fit Index
PII	Personally Identifiable Information
PIN	Personal Identification Number
PMBs	Primary Mortgage Banks
PMT	Protection Motivation Theory
POS	Point of Sales
PS	Profile Score
QUAL	Qualitative
QUAN	Quantitative
RAM	Random-Access Memory
RAT	Routine Activity Theory
RFI	Relative Fit Index

RMR	Root Mean Square Residual
RMSEA	Root Mean Square Error of Approximation
SEM	Structural Equation Modelling
Smart TV	Smart Television
SPSS	Statistical Package for the Social Sciences
SSL	Secure Sockets Layer
TA	Thematic Analysis
TO	Time Out
TLI	Tucker-Lewis Index
UK	United Kingdom
ULS	Unweighted Least Squares
URL	Uniform Resource Locator
USA	United States of America
USB	Universal Serial

CHAPTER ONE: INTRODUCTION

1.0 Introduction

With the global use of progressively more sophisticated internet and information technology (Papazoglou, 2003), electronic banking is developing as a key channel for banking businesses (Wei et al., 2012). Globally, remote banking is regarded as a characteristic of the new economy, which involves electronic transactions between banks and their customers (Banstola, 2007). Electronic banking, generally referred to as e-banking, is the latest delivery channel for the banking system (Keivani et al., 2012). The term "e-banking" has been discussed in several ways by many researchers from diverse backgrounds, mostly because electronic banking involves quite a lot of banking activities through which customers can inquire for financial information and implement transactions by means of a digital television, telephone, mobile phone or computer (Hoehle, Scornavacca & Huff, 2012). Perkins and Annan (2013) describe electronic banking as the rendering of services and dissemination of information by banks to customers through various delivery channels that can be accessed with a personal computer or other electronic devices.

However, the banking sector is being reformed by globalization, innovation, customer needs and competition. Due to the development of a knowledge-built economy and the emergence of the latest information and communication technology, financial institutions particularly the banking industries have experienced thought-provoking changes during the last decade. According to the Wisdom (2012), Information and Communication Technology, the most significant factor in the forthcoming development of the banking industry, enhances banks' ability to produce sophisticated products, to have superior market structures, to diversify their markets and to expand globally. Furthermore, Darlington (1999) states that over the past three decades, customers' needs have changed

significantly: customers are demanding simplicity in their daily banking services together with maximum security and safety.

Thus, the traditional banking system, which consists of physical branches, is now being threatened by information and communication technologies characterized by automated systems of interaction with customers (mobile banking, call centres, automated teller machines (ATMs), online banking), that include relatively minimal costs and permit customers to select from the alternative delivery channels (Keivani et al., 2012). Therefore, electronic banking has become a great business; the transformation from traditional banking to electronic banking has been a "Leap" change (Yazdanifard, WanYusoff, Behora, & Abu, 2011; Wang & Huang, 2011).

Globally, the electronic banking system addresses several emerging trends: it is very convenient and easy for electronic banking users to manage and access their bank accounts at any time and from anywhere in the world (Brar, Sharma & Khurmi, 2012). The banking sector has been strengthened by this development in recent years, since electronic banking saves vast amounts of resources in areas such as investments into ATMs, staff training, opening of branches and other operational costs (Chaturvedi & Meena, 2016). The internet has improved users' experience of electronic banking operations dramatically (Abu-Shanab & Matalqa, 2015). Banking transactions can now be performed any place, anytime in the world through any bank delivery channel: ATMs, POS, Smart TV, personal computers, telephones are among the channels a customer might consider (Hoehle, Scornavacca & Huff, 2012).

E-banking is the significant application of the internet for banking activities, and bank sectors have upgraded their business strategies with the assistance of the internet. Banks have provided their services via the internet and thereby electronic transactions have increased speed in the banking industry worldwide (Mahdi, Rezaul & Rahman, 2010). The advancement of electronic transactions gives a tremendous prospect for benefits to consumers and financial institutions (Singh & Singh, 2015).

Corroborating this, the emergent modern technologies have resulted to significant transformation of banking approaches and techniques. Bank branches have started to lose ground to computer-generated banking as the use of distant banking services has been augmented (Hoehle, Scornavacca & Huff, 2012). Globalization, transforming social trends, competition and particularly information and communication technology advancements have brought intense reform of the banking system (Loonam & O'Loughlin, 2008). Generally, information infrastructure is considered worldwide as an opportunity for introducing innovative electronic distribution channels for bank products and services.

In contrast, fraudulent electronic activities are increasing and becoming sophisticated, severely threatening and menacing the trust and security of electronic banking services (Mahdi, Rezaul & Rahman, 2010). E-banking fraud has turned into a thoughtful and serious phenomenon to the financial fraud and crime management in the banking industry across the entire globe (Rajdeepa & Nandhitha, 2015). These current electronic fraud opportunities are often tremendously difficult to mitigate due to their technological complexity; hence, banks may devote substantial resources endeavouring to prevent and detect them (Kranacher, Riley & Wells, 2011). Banks encounter challenges in preventing and detecting fraud, and these challenges can often be aggravated by the organizational frameworks, political frameworks, regulatory frameworks and newly invented technology approaches that are in place. Nevertheless, even the issuing of momentous regulatory frameworks and the regulatory supports of a given economy or nation cannot be predicted to eliminate or minimize the occurrence of fraud in the banking sector (Hoffman, 2002). However, in the very beginning of electronic banking systems, the scale of fraud was very insignificant because the banking industry was one of the most strictly regulated sectors, which treats prevention of fraud as a duty (Mahdi, Rezaul & Rahman, 2010; Shannak, 2013).

On the contrary, banking represents the mediator of the economy; fraudulent acts have brought enormous losses that are affecting all the performing activities (Sahin &Duman, 2010). Equally, banking development, from traditional banking to electronic banking, is

not only challenging in terms of managing bank risk, but also with international and national irregularities (Saranya & Gunasri, 2013; Chaturvedi & Meena, 2016; Abu-Shanab & Matalqa, 2015).

Conversely, the findings also supports the issues that the factors contributing to the increase in e-banking fraud in Nigeria include ineffective banking operations, internal control issues, lack of customer awareness and bank staff training and education, inadequate infrastructure, presence of sophisticated technological tools in the hands of fraudsters, negligence of banks' customers concerning their e-banking account devices, lack of compliance with the banking rules and regulations, and ineffective legal procedure and law enforcement. In addition, the enforcement of rules and regulations in relation to the prosecution of financial fraudsters has been passive in Nigeria. Theses also corroborated with diverse types of security threats for both the electronic banking users and the banks – such as distributed attacks, phishing, identity theft, brute force attacks, spamming, credit card frauds, ATM frauds, hacking and unauthorized access, theft of service frauds, online money laundering, denial of service attacks, creation and distribution of malware attacks and other related online frauds – are challenging issues.

However, e-banking fraud has created an aggressive presence in the banking sector and therefore, security cognizance is required in order to bring behavioural transformation, minimize employees' vulnerability and guard against the prospective risk of fraud; and to create strong detection and prevention of fraud using electronic technology, adoption of fraud awareness and other new sophisticated anti-fraud approaches. Hence, to cover these gaps there is a need to examine the natures, contributing factors, preventive and detective mechanisms of e-banking fraud.

1.1 Background of the Research Problem

The banking sector globally plays an essential role in advancing the smooth growth of economic activity (Sruthi & Prasanna, 2016). As intermediaries between users and suppliers of funds, banks are successfully placed in a continuum that controls the pulse

of the economy (Rampini & Viswanathan, 2015). Globally, the incapability of the banking sector to effectively perform its functions as intermediary and inability to control financial challenges that are experienced hitherto have been a crucial concern (Gertler & Nobuhiro, 2010). Equally, Rampini and Viswanathan (2010) state that the main attribute of banking industry businesses is to perform as deputized monitors and adviser of borrowers on behalf of legitimate depositors.

However, in this special association with borrowers and depositors, banks need to protect the confidence and trust of their various clients (Wei et al., 2012). The failure of banks to satisfactorily perform their role resulted from the numerous risks they are exposed to which are not appropriately controlled (Papazoglou, 2003). One of these risks which are progressively becoming a cause of burden is the banking risk related to fraud (Sruthi & Prasanna, 2016). Furthermore, fraud, which literally means an intentional act of deception that makes society suffer damage, either by monetary or physical asset losses, is now a global menace to the entire banking industry (Ramamoorti, Morrison & Koletar 2013).

Respectively, it is truly bothersome that while the banking sector is persistently trying to contend with the demands of monetary authorities to recapitalize up to the required minimum standards, fraud perpetrators are always at work decimating and threatening banks' financial base (Mahdi, Rezaul & Rahman, 2010). Also, the worrisome issue in Nigeria is the extent of involvement in the act of e-banking fraud by bank management staff and collusion with outsiders, as well as the ease with which many elude detection, hence inspiring many others to cooperate in perpetrating fraud (Usman & Shah, 2013).

In the same vein, according to Mannan and Oorschot (2008), the consistent of fraud incidents in the banking sector has currently become discomfiture and disconcertment to the country, as is obvious from the apparent incapability of the anti-fraud agent and other law enforcement agents such as police to effectively get hold of the perpetrators. Statistics on the impacts of fraud perpetrators in the banking institutions are both confounding and amazing. Akindele (2011) predicted that on average, the bank sector in Nigeria was at a

risk of losing a million Naira every working day because of the occurrence of frauds, which happen in diverse ways.

Correspondingly, this estimation is low compared with the Nigeria Electronic Fraud Forum (Neff) (2016) report, where banks reported the vast amounts of ₦485,194,350 (£1,239,488) being lost to fraudsters in 2013 and ₦6,215,987,323 (£15,879,491) in 2014 with 822 and 1461 cases in each year respectively. Also, a report by NeFF (2017) shows that a total actual loss of ₦2.19 billion (the equivalent of £4.88 million) was recorded by Nigerian Deposit Money Banks (DMBs) in 2016. This was broken down into ₦511.1 million (£1.12 million) of value lost across counter, ₦464.5 million (£1.03 million) lost to ATM fraud, ₦132.2 million (£0.29 million) to e-commerce fraud, ₦320.6 million (£0.71 million) lost to internet banking, ₦235.1 million (£0.52 million) to mobile banking, ₦243.3 million (£0.54 million) to POS, ₦83.7 million (£0.19 million) to web fraud, ₦10.1 million (£0.022 million) value to Kiosk fraud, ₦4.54 million (£0.03 million) to cheque fraud and ₦190.9 million (£0.42 million) to other losses.

These reports also testified that fraud contributed greatly to the failures of most banks in Nigeria. Even with the efforts of the Independent Corrupt Practices and Other Related Offences Commission (ICPC) and the Economic and Financial Crimes Commission (EFCC), which were introduced to combat fraud at various levels in Nigeria, it is regrettable to witness that little or nothing has been achieved (Aibieyi, 2007).

Moreover, presently fraud in the Nigerian banking industry is not properly investigated by the Central Bank of Nigeria, and therefore there is no enough information regarding challenges of e-banking fraud incidences, prevention and detection, and insufficient research studies on this phenomenon. This has become a controversial issue which generates debate among quite a few authors, for example Chaudhary, Yadav and Mallick, (2012); Mahdi, Rezaul and Rahman, (2010); and Sruthi and Prasanna (2016), who have investigated similar phenomena.

However, their studies examine only causes of credit card frauds and not mobile fraud, online fraud, computer base fraud and telephoning fraud, which are major channel

services of electronic banking, even without discussing the prevention and detection aspects of fraud. Also, most studies done earlier in Nigeria on fraud have employed secondary data and did not consider the use of primary data, while employees were the main focus of those studies. Thus, an innovative approach is required to mitigate e-banking fraud. Therefore, these acknowledged gaps provide the motivation for this present study.

1.2 Aim of the Study

The research of Nwankwo (2013), a study of internet banking fraud in Nigerian banking sector, indicates that fraud in the Nigerian banking sector negatively affects bank performance, profitability, operational efficiency, foreign direct investments, credibility and reputation. It also causes a psychological and emotional burden on the victims of fraud, criticisms in the public arena and a bad national image. However, it is obvious that, today, no nation in the global economy can sustain business transactions without e-banking. Therefore, there is a need to improve the image of the Nigerian economy in the sight of local and foreign investors. Hence, the current research aim is to examine e-banking fraud detection and prevention mechanisms in Nigerian banking sector.

1.3 Research Questions

The following research questions have been framed to address the research aim:

1. What are the e-banking fraud risks that are of high concern in the Nigerian banking sector?
2. What are the perceived factors that have considerable influence on the increase in e-banking fraud in Nigeria?
3. What are the current significant mechanisms for e-banking fraud prevention in the Nigerian banking industry?
4. What are the current significant mechanisms for e-banking fraud detection in the Nigerian banking industry?

1.4 Scope of the Study

This study concentrates on the deposit money banks (commercial banks) in the Nigerian economy; the research questions were used to ascertain the effect of e-banking fraud on banks' stockholders, and its prevention and detection. The study covered the activities of both internal and external stakeholders of commercial banks in the Nigerian economy, since the core function of both internal and external stakeholders is to ensure an effective use of the e-banking system. Data were collected from accountants, internal auditors, external auditors, managers, and directors who are working in the head offices of Nigerian commercial banks and also customers within the banking premises by the use of questionnaires and direct interviews. The selection of the head offices is to facilitate the study by covering those internal and external bank stakeholders who have common experience within the financial sector of the Nigerian economy.

This study was carried out to show detailed appraisal of e-banking fraud detection and prevention and to enable the researcher to provide appropriate answers to the fundamental questions raised in this section, which subsequently form the basis of the research objectives. However, there are also difficulties with the gathering of dependable historical data of fraud occurrences, where most incidences of fraud go undetected (Wells, 2014). Thus, the scope of this research is constrained to only licensed deposit money banks in Nigeria at the time of this research.

1.5 Rationale for the Research

Over the past two decades, fraud has increased both in complexity and magnitude. The costs of fraud are increasing globally. Studies in the USA and the UK indicate that the loss through fraud continues to increase daily (ACFE, 2015; KPMG, 2000). In Nigeria, NIDC (2012) cited fraud cases related to identity fraud, internet banking fraud, bank card

fraud, ATM fraud and fraud through phishing and pharming that were reported in Nigerian deposit money banks. These totalled 3,380 of fraud cases in the year 2012 with the sum of ₦17.97 (£9.97) billion. The contingent or expected loss was greater by ₦455 (£234) million (10.9%) in 2012 than the ₦4.072 (£2.072) billion disclosed in 2011 with the cases of 2, 352. However, the report of the African Fraud and Misconduct survey indicates that a loss of US$170,000 was sustained in 2001 from internet frauds, ATM frauds and bank card frauds.

Therefore, the current research aim is to examine e-banking fraud detection and prevention mechanisms in Nigerian banking industry in order to provide information on the challenges of e-banking fraud incidences in the Nigerian banking industry, as well as dialogue on what the banks are doing to prevent and detect e-banking frauds. It provides useful information for foreign organizations considering participation in the Nigerian economy. This study also gives insights on how to advance Nigerians' access to global investment funds.

1.6 Significance of the Research

The current research has significance for theories and empirical applications in the areas of policymaking and financial institutions. Theoretically, the submission of prevailing theories of frauds, such as routine activity theory (RAT) (Cohen & Felson 1979; Williams, 2016) and fraud management lifecycle theory (FMLT) to the Nigerian e-banking fraud prevention and detection context will generate more information about whether these theories can be applied worldwide or whether they depend on cultural or local structures.

The research can likewise be projected to expose some of the prerogatives that are claimed in the academic and theoretical literatures regarding the understanding of fraud in the financial context and its connotation. Given the application of present theories along with other information from the research concerning the Nigerian banking sector, this can be regarded as significant research from this viewpoint.

There are also substantial practical applications of this study. The Nigerian banking sector can use the information generated from this study to modify its practices of combating fraud, and in addition to identify areas that are performing well. Investors and customers are the major users of this information in a practical mode. One of the challenging factors is overseas investment fraud (Broadman & Isik, 2007). However, to some degree, financial risk is essential in almost all financial institutions. Understanding the level of risk and the specific factors that will need to be overcome will be tremendously significant for investors to make suitable decisions.

Moreover, the findings of the current study will be of interest for legal, regulatory and law enforcement institutions and policymakers within the executive and legislative arms of the Nigerian government; executive directors of Nigerian financial institutions; and all professional accounting and banking bodies. Also, corporate financial institutions will be able to design better control systems to curb fraudulent practices within their operations. The study will identify exposure to e-banking fraud and appropriate prevention, detection and investigation approaches which will enhance national economic development, as the banking sector constitutes the backbone of the country's economic activities.

Finally, even though several studies have been conducted on e-banking fraud in various parts of the world, particularly in the United Kingdom and United States of America, no broad study has been done in Nigeria, where the information that exists is piecemeal. It is therefore expected that this study will contribute significantly to the literature of the existing body of knowledge on e-banking fraud and on the developing economy.

1.7 Structure of the Thesis

The structure of the thesis is presented as follows:

Chapter 1 comprises an introduction to the study. It sets out the background of the study, the aims and research questions. It also presents the scope, rationale and significance of this study.

Chapter 2 presents the literature review of the thesis. The thesis focuses mainly on an examination of e-banking fraud detection and prevention in Nigerian banks. The chapter discusses the contextualisation of the Nigerian banking system, history of Nigeria banking system and constructs of electronic banking, it also elucidates the impact of e-banking fraud, e-banking attacks and techniques and the contributing factors to the increase of e-banking fraud. The discussion also includes e-banking fraud detection and preventive mechanisms while ending with a summary.

Chapter 3 elucidates the two principal theories of criminology and management adopted as theoretical frameworks that underpinning the study, which are the routine activity theory (RAT) and fraud management lifecycle theory (FMLT).

Chapter 4 explains the methodology and methods adopted for the research design by discussing research in philosophy which involves the epistemological position, the ontological position, axiology positions and postmodernism. It extensively describes the application of triangulation in this research design. It also explains population, sampling strategy, research instruments design and testing data collection procedure for this study. Data preparation and analysis, procedure factor analysis, structural equation modelling (SEM) validity, ethics in research and a summary are obviously discussed also.

Chapter 5 discusses quantitative analysis, which elucidates the outcomes of the survey analysis that was conducted, the major purpose of conducting the survey, factors for the increase in e-banking fraud, and current prevention and detection mechanisms in the Nigerian banking system. It includes the demographic information of the respondents.

Chapter 6 discusses the qualitative research which was based on the research methodology. This chapter deliberates on the analysis of data collected through the survey interviews. Section 6.1 describes the demographics of the interviewees; section 6.2 offers a brief elucidation of the analytical tools (that is, thematic analysis and content analysis) chosen for interpreting the face-to-face interviews conducted with ten corporate executives of selected commercial banks in Nigeria.

In addition, the chapter also discusses the findings and integrates the quantitative and qualitative findings of this research work with the present literature to understand e-banking fraud in the Nigerian banking sector. In this chapter, the nature, contributing factors to the increase of e-banking fraud in the Nigerian banking industry, and its preventive and detection mechanisms were harmonized with the research questions.

Chapter 7 is all about conclusions and recommendations. It elucidates the practical and theoretical contribution made in this study, summarizing the major findings in respect of the research questions, explaining contribution to literature, theory, and knowledge, revealing policy implications and providing recommendations. Finally, this chapter concludes with the explanation of limitations to the study and discussion of areas for upcoming research.

CHAPTER TWO: LITERATURE REVIEW

2.0 Introduction

The core focus of this chapter is to present the literature review of the thesis. The thesis focuses mainly on an examination of e-banking fraud detection and prevention in Nigerian banks. The chapter discusses the contextualisation of the Nigerian banking system, history of Nigeria banking system and constructs of electronic banking, it also elucidates the impact of e-banking fraud, e-banking attacks and techniques and the contributing factors to increase of e-banking fraud. The discussion also included e-banking fraud detection and prevention mechanisms while ending with a summary.

2.1 Contextualisation of The Nigerian Banking Systems

The Nigerian banking sector is one of the momentous sectors that are contributing to the development of the economy in Nigerian. Over the decades, banking system in Nigeria has achieved incredible growth and development in activities and structures. This section focuses on contextualising of the Nigerian banking sector, which comprises its history, evolution and structure of the Nigerian banking system.

2.1.1 The History of Nigeria Banking System

The history of the Nigerian banking industry dated back to the colonialism epoch. The colonial banks were established by the colonial government to accomplish its commercial purpose. African Banking Corporation and British West Africa bank were established in 1892 as the leading banking industries in Nigerian. Thereafter, they were amalgamated and formed present First Bank of Nigeria (Ezeoha, 2007).

In 1925, Barclays Bank was established through the joining of Anglo-Egyptian Bank and National Bank of South Africa (CBN, 2014). The British and French Bank for Commerce and Industry started business operation in 1948 which later modernised and reformed into the existing United Bank for Africa. The first local bank was established in 1929 which called Industrial and commercial bank but collapsed in 1930.

However, after the collapse of the first indigenous bank, the Nigeria Farmers and Commercial bank were established in 1947 for agricultural growth and development. Followed by the Continental Bank, which came into inception in 1949. (Okoh & Okoh, 2014). The central bank of Nigeria (CBN) is an autonomous bank that controls and supervises the monetary and fiscal policies for the Nigerian government as well as oversees the Nigerian banking system. (Central Bank of Nigeria, 2009).

Central bank of Nigeria was founded in 1958 before political independent on the 1st October 1960 through the CBN Act in 1958 and started operations on 1st July 1959 (CBN, 2002). The central bank of Nigeria is the regulatory authority of the banking sector in Nigeria. It is generally known as the leading monetary authority and the central issue of legal tender in Nigeria (CBN, 2014).

Amongst its core functions, the central bank of Nigeria encourages monetary constancy, price stability, banking industry, dependability and of course, financial and banking adviser to the Government. Besides this, the Bank also enhances the development and advancement of banking institutions. Enabling laws enacted in 1991 offered the Bank more suppleness in licensing, overseeing and regulating the banking industry and other finance systems (Central Bank of Nigeria, 2017).

However, since 1959 when the Central Bank of Nigeria (CBN) established has been playing its role as the apex of Nigerian banking authority. Despite the issuance of legal tender, Central Bank of Nigeria performs significant impacts in regulating the economy in Nigeria and modifying the structure of the Nigerian banking system.

2.1.2 The Structural Reform of Nigeria Banking System

The Nigerian banking system has experienced main current banking reforms that have had a substantial impact on the Nigerian economy. The first Nigerian banking system reform took place in 2004 while the subsequent banking system reform was performed in 2010 (Sanusi, 2011).

The 2004 banking system reform focused on the combination of banks by means of merger and acquisition, which replaced deposit money banks to ₦25 billion minimum capital base from ₦2 billion and minimized the number of banks to 25 from 89 in 2005 and further to 24 (Sanusi, 2011). The aim of this reform was to strength and position the banks play crucial roles in bringing advancement and expansion across the segments of the national economy. While, the Asset Management Corporation of Nigeria (AMCON) was introduced in 2010, subsequent by the announcement of its empowering Act through the National Assembly. It is significant purpose was to address the challenges of non-performing loans in the Nigeria banking sector (Kolapo, Ayeni, & Oke, 2012; Sanusi, 2011).

Corresponding to the AMCON mandate, AMCON currently takeover of the non-performing loan of certain banks valued over N1.7 trillion, which supposed to boost their soundness and safety as well as increase their liquidity. With the involvement of the AMCON, the ratio of non-performing loan in the Nigerian banking industry to gross credit has significantly low from 34.4% to 4.95% as at December 2011 (Agbada, & Osuji, 2013). Furthermore, the central bank of Nigeria and all the commercial banks or deposit money banks in Nigeria signed an MOU to finance the AMCON in order to accomplish its mandate. The central bank of Nigeria contributes ₦50 billion every twelve months to AMCON while, each of the participated deposit money banks pays 0.3 percent of their total assets per annum to the sinking fund. Therefore, the resolution cost to the taxpayers in Nigeria is significantly diminished (Kolapo, Ayeni & Oke, 2012).

Moreover, in 2011, the Nigeria Incentive Risk Sharing System for Agricultural Lending (NIRSAL) was introduced and incorporated in 2013 by the central bank of Nigeria

(CBN). The NIRSAL was incorporated to build credit facility and capacity of the banking industry to engage and provide loans for agriculture by producing technical support and minimising counterpart threats facing banking institutions (Anyanwu, 2010). In 2008, due to the challenges caused by fragmentation and weaknesses of the financial sector, the central bank of Nigeria introduced a guideline named "The Project Alpha Initiative" to reform banking sector and other financial system in general. The reforms designed to stop the inherent fragmentation and weaknesses of the financial system, banking system, integrating the different, piecemeal and ad-hoc reforms and releasing of the huge strength of the economy (Sanusi, 2011).

To address the identified crises, the central bank in 2010 revisited the universal banking model by guiding banking industries to concentrate on their fundamental banking activities which they licenced for. Under the current guideline, licensed banks were approved to perform banking activities of their license category (AJAYI, et al. 2018).

However, the licenses of the Nigerian banking system have been grouped into three categories in relation to their activities, namely:

1. Commercial Banking (Deposit Money Banks) License
2. Merchant Banking License
3. Specialized/Development Banking License

As at 31st December 2016, the Nigerian banking industry made-up of 28 banks, which comprised of 22 deposit money banks (DMBs) that was previously known as commercial banks, 5 merchant banks and 1 non-interest-bearing bank (CBN, 2017).

However, the Nigerian deposit money banks, which comprise of 22 banks of 3978 branches all over Nigeria hold 78% of the capital reserves, total net assets and also, share over 83% of total profitability in the banking sector, while the remaining 22% of the capital reserve and total net asset, including 17% of the total profitability in the banking sector are shared by the other 6 banks (5 merchant banks and 1 non-interest-bearing bank (CBN, 2017). In addition, there are other institutions in the Nigerian financial system that will not be investigated in this study include bureaux-de-change, development, financial institution, discount house, finance company and primary mortgage banks (Sanusi, 2011).

Furthermore, in 2014 introduction of Bank Verification Number (BVN), globally, biometric technology has been adopted to analyse human characteristics as an improved form of verification, authentication and certification for real-time security methods (Blass & Oved, 2003). In the face of cumulative occurrences of compromise orthodox security systems (PIN and password), the need for sophisticated security on access to personal and sensitive information in the Banking industry becomes inevitable. Therefore, the Central Bank of Nigeria through the Banker' Committee and in cooperation with all banks (Deposit Money Banks (DMB) and Nigeria Interbank-Settlement System (NIBSS)) in Nigeria on February 14, 2014 introduced a centralized biometric identification system for the banking sector marked Bank Verification Number (BVN) (CBN, 2014).

The BVN project was introduced due to growing incidents of compromise on conservative security systems (PIN and password) and an increase demand for sophisticated security for sensitive information in the Nigerian Banking System. However, the aim of this project (BVN) is to prevent bank customers from identity theft and other financial frauds emanating in the Nigerian banking industry (Orji, 2015). The current research will analyse the present mode of operation in the Nigerian banking industry comprising its impacts since the date of introduction in the Nigerian electronic banking system.

2.1.3 Evolution of Electronic Banking in Nigeria

In the few years, past, Nigerian financial institution, particularly banking industry incorporated electronic banking, through the help of development of information technology. The Allstate Trust bank was the first to introduce e-payment in 1996 through the approval of the Central Bank of Nigeria to introduce a close system, electronic purse called Electronic Smart Card Account (ESCA) (Imala, 2002; NIBSS, 2015). The introduction of Pay card, followed in 1997 by Diamond Bank with the authorization in February 1998, this e-money product card open platform of Smartcard Nigeria Plc Which established by a group of 19 banks to manage and produce cards known as "Value card" and used by the member banks. Between 1999 and 2002, many banks launched their

websites with the aim of starting electronic banking. In November 1999, another group of 20 banks in the Gem card Nigeria limited got the Central bank of Nigeria approval to introduce the "Smart pay" scheme. As from 2002, many banks have been given the approval by the central bank of Nigeria to introduce telephone banking, international money transfer and electronic banking through a limited level (Imiefoh, 2012; Chiemeke, Evwiekpaefe & Chete, 2006; Ezeoha *2005).*

A lot of sophisticated on-line banking products were, thereafter, introduced to enhance better delivery and customer satisfaction. According to Central Bank of Nigeria 2003, "Automated Teller Machine; Personal Computer banking; Cards, Telephone Banking and On-line Banking is now available in Nigerian banking system". Correspondingly, the study of the range of electronic banking approval and implementation by Nigerian financial institutions, the Central Bank of Nigeria (CBN) (2002) disclosed that out of the 89 licensed banks that were available in the nation, 17 were operating online banking, 24 were operating telephone banking, while 7 had started an Automated Teller Machine system, and 13 were operating other types of electronic banking.

As of 2002, it indicates that the average Nigerian bank was operating at least one form of electronic banking; thus, indicating that electronic banking was yet to operate at full range, regardless of its extensively acclaimed aids in compared to traditional banking firms (Ezeoha, 2005). Therefore, Nigerian banks today are extremely into new on-line delivery channels for electronic banking services and products with the aims of better performance in servicing and satisfying customers**.** The Nigerian banking industry has advanced from traditional services to electronic banking (Salu, 2004; Oghenerukevbe, 2008). Gorman (2006) agreed that banks gained a hundred and seven times of total cost as soon as electronic banking was adopted. It's all time accessibility makes it suitable for the banks' customers. Nigeria as any developing nation is not up till now to be seen at this stage and therefore cannot be found with similar levels of banking services like Western societies or developed countries. For instance, more than an average of populace in Nigeria, is not banked and transaction electronically. (Kanu and Okorafor, (2013); Igbaekemen, Abbah and Geidanm (2014).

Nigerian banks have in the recent past reorganization transmuted from manual systems to automated systems. Ogbuji, Onuoha, and Izogo, (2012) in the research titled "Analysis of The Negative Effects of the Automated Teller Machine as a Channel for Delivering Banking Services in Nigeria" paper-based payment instruments have been replaced with an automated means of payment in Nigeria, thereby enabling the use of electronic banking transactions.

The current adoption of mobile telephone system in Nigeria has enhanced the use of personal computers and internet service facilities to facilitate the progressive use of electronic banking and to enhance cashless era. The low rate of electronic banking services in Nigeria is emanated from the high proportion of illiterates and electronic banking fraudsters' activities in the country (Owolabi, 2011). Also, asserted by Uchenna and Agbo, (2013) that participating of the customers in this new process of electronic banking in Nigeria is far from being achieved as a result of internet fraud and lack of adequate regulatory framework for prevention and detection.

Conversely, increasingly over the years, Nigerian banks have observed a lot of institutional reforms and regulatory. Just of recent, The Central Bank of Nigeria introduced reforms by looking at decreasing the number of banks in the nation and building the emerging banks to be much more dependable and stronger. This occurred through great challenges faced by the banks in Nigeria such as: corruption, inadequate capital base and asset quality, loss in public confidence, fraudulent practice (Fatokun, 2016). Therefore, with the aim to compete with the global financial economy and to advance the quality of their performance delivery, Nigerian banks must invest enormously on security to escape from the menace of the fraud.

2.2 Concept of E-Banking Fraud

Numerous definitions of fraud have been advanced in the crime literature. Wells (2014) defined fraud as unlawful gain through deception. Taylor (2011) argued, in line with Wells, that fraud is stealing, disguising and obtaining personal gain from another person or a group of persons through deception. Curt's (2013) noted that fraud contains the

acquisition of property or monetary advantage by way of deception, either concealment or misrepresentation. Boniface (1991), agreeing with the above three authors, described fraud as any deliberate act of illegal deceit, scam or forgery by a group of persons or a person with the aim of modifying facts to gain unjustified personal economic benefit. According to Graycar and Smith (2002), frauds usually encompass the transaction, falsification or forgery of financial documents and unlawful endorsement.

KPMG (2000) observed that fraud occurs when a person or a group of persons of authority and responsibility refuse standard and violate the rules for the benefit of self-interest at the expense of others. Mirjana Pejic-Bach (2010), opined that fraud is misrepresentation of financial records by an individual or group of individuals among employees in the management of an entity or third parties.

In 1888, the United States Supreme Court accepted that fraud happens when there is a misrepresentation of a material fact by the defendant and the complainant sensibly believes it to be true. Entities, either as individuals or organizations, commit fraud to get a monetary advantage (Silverstone & Sheetz, 2004). Hence, fraud is criminal offences using deception for personal gain to the disadvantage or loss of another person. It comprises activities such as deception, concealment theft, money laundering, bribery, forgery, corruption, embezzlement, conspiracy, misappropriation, collusion, and extortion of material facts (CIMA, 2009).

Furthermore, from the above definitions, fraud can be described as a deception and a false channel for converting another person's (legal owner) financial and non-financial property/assets for personal interest illegally. It can also be explained as a misrepresentation of financial statement which is intentionally done by internal or external stakeholders of an organization for personal motives. Bank fraud, then, involves the deceitful use of one's position without or within the bank for self-enrichment by intentionally misappropriating the bank's financial means, properties, or other resources held by the bank and collecting funds from bank accounts of customers (Taylor, 2011).

Now what, then, is e-fraud? According to Graham (2008), electronic fraud is a fraudulent act associated with an automated system by which someone aims to gain fraudulent benefit. The USA Department of Justice described the electronic fraud in the internet perspective as “a fraud system that adopts internet components such as emails, Web sites to existent fraudulent solicitations to potential victims, Web sites, to perform fraudulent transactions, to transmit the proceeds of fraud to banks or to others connected with the scheme” (Finch, 2010).

The differences in the definitions of e-fraud are attachable to certain factors such as the varied contexts in which e-fraud has been found to occur. Therefore, electronic banking fraud can be elucidated by the researcher as theft, robbery, forgery and altering of another person’s financial assets illegally for self-motivated ends with the help of the internet. Electronic banking fraud can also be illuminated as a deception and dishonest way of converting another person’s monetary advantage for personal benefit at the expense of others with the use of electronic devices and the internet.

2.3 Panaches of Perpetrating Banking Fraud

Again, literature is satiated with distinctive styles of frauds. This view has been debated amongst scholars. Hamilton, Justin and Odinioha (2012) in the study titled, “styles of fraud are usually not exhaustive as fraudsters are forever devising new methods.” Therefore, as societies and businesses are expanding as progressive techniques of committing frauds are sophisticated and classy (Pedneault, Sheetz & Rudewicz, 2012). The growth of businesses and rapid increased of the fraud perpetration are as a result of the development and expansion of the communication and information technology (Silverstone and Sheetz 2007).

Furthermore, Udoayang and James (2004) opined that fraud could be seen in two ways, viz. bite and nibble frauds. When an individual taken assets and disappears in order to not be detected is known as bite fraud. This style of fraud usually involves stolen of large assets or huge amount of money and can be easily detected. To escape being detected and tracked down, the fraudster breaks out into a protected colony. Bite fraud can occur in the

form of electronic frauds particularly, stealing of hardware devices or back-up devices of a computer system. While, an individual or fraudster involves in taking assets in piecemeal or small unit in order to not be detected easily is called nibble fraud. This style of fraud is very difficult to be detected at an early stage, hence, this kind of fraud occurs every day and is common in electronic banking frauds, particularly, fraud through ATM, PoS, credit card and web banking fraud.

Moreover, Alao (2016) grouped fraud styles into two, internal fraud and external fraud. When fraud is perpetrated by the individual employee or group of employees of an organisation or a bank using computer, point-of-sales, automated teller machine and internet inform of phishing, vishing and counterfeited or forged smart card is recognized as internal fraud. While, fraud committed with the use of bank financial records, customer's financial information and electronic devices such as ATM, internet, mobile app, mobile phone, pocket picking machine by the outsiders, such as service providers, bank customers, suppliers and unknown party is called external fraud (Hansen et al 1996; Sydney, 1996; Adewumi, 1986). Iwuagwu (2000) argued that, fraud perpetration can involve combination of both internal and external which known as outsider-employee fraud. This kind of fraud is difficulty to detect because the insider-fraudster is supplier of financial information needed and bank security information carrier to the outsider-fraudster who is an operator of fraudulent acts.

Additionally, Association of Certified Fraud Examiners, (2015) argued that fraud against a business organisation can be perpetrated either externally by vendors, customers and other related parties such as individual or managers, employees, officers, and owners of the organisation. The author categorised frauds into three basic categories which are: external frauds, internal frauds and frauds against individuals.

External frauds are kind of frauds committed by outsiders or third-parties by compromising electronic bank account through personal information about the victims. This fraud could happen through pharming, phishing and vishing. While, internal frauds also known as occupational frauds, can be explained as a means of using one's profession or occupation for self or personal gain through intentional misuse or misappropriation of

the company's resources. This kind of fraud happens when the executives, managers and other employees perpetrate frauds against their employer.

Iwuagwu (2000) further argued that, fraudsters are progressing in the use of technologies and innovative approaches for concealment and perpetration of internal fraud schemes. While, fraud against individuals is a type of fraud in which many perpetrators have designed systems to defraud individuals such as identity theft systems, phishing systems, advanced fee crimes are just a few of the methods the fraudsters have discovered to defraud unsuspecting victims.

On the same vein, Adeyemo, (2012) opined that, fraud has been categorised in diverse ways and using various methods such as management and employee frauds, customer and non- customer frauds and stakeholder and non-stakeholder frauds. Management Frauds are electronic fraud perpetrated by the top management of the organisation. These frauds can be committed through electronic financial statement and the group of sufferers of these kinds of frauds are creditors and investors (Association of Certified Fraud Examiners, 2015). This electronic banking fraud can be perpetrated through the creating of more investment from potential and current shareholder of the organization, Doctor of Financial statement or window dressing of account statement and can occur by painting the bank in better light in the eyesight of the regulatory authorities using electronic systems.

Kevia & Huange, (2011) explained that management fraud as the falsification of financial statements for the benefit of the person perpetrating the fraud. This involves false transaction, bogus trades, backdating of executive security or stock trade options and wrong use of corporate asset for personal benefits and violation of tax rules and regulations for personal gain using the internet and electronic devices.

While, Association of Certified Fraud Examiners (2012) concord that management frauds happen through timing differences, fictitious revenues, improper asset valuation, inadequate disclosure and concealed liabilities and expenses. Employees' Fraud is generally known as non-management fraud. It is a kind of fraud committed by the non-management staffs or employees of the organisation through forgery of customers'

signatures, stealing of customer's passwords, PIN codes and electronic cheques for illegal withdrawal of money from the customers' accounts, creating and operating of fictitious electronic bank account, fund diversion, lending fictitious borrowers and other related computer's fraud or internet frauds (Adeyemo, 2012).

Furthermore, customers and Non- customers' frauds occurred through the act of performing the primary functions of money deposit Banks, which connects capital deficit customers with the capital surplus customers in the money market (Association of Certified Fraud Examiners, 2012). In the process of this, bankers come in connecting or interacting with both non-customers and customers and this leads to the risk of frauds. These types of frauds may be through counterfeit securities, opening of the fictitious electronic bank account, forged electronic cheque, fraudulent electronic money transfer because of a request made sole and solemnly through email, telephone, fax, telex, and other electronic means, and skimming card data (Regha, 2015).

While, stakeholders' and non- stakeholders' frauds is the kind of fraud perpetrated through the collaboration of insiders and outsiders, employees and non-employees, staffs and non-staffs of the organisation. Before this type of fraud to succeed, there must be an insider or internal fraudster that will be providing financial information while, the outsider fraudsters or external fraudsters will be carrying out the instruction given Adewunmi (1986). However, majority of banking functions in Nigeria are now electronically base activities including transaction of business such as funds, registration of new customers, collection of customers' personal data and preparation of financial statements, particularly in this era of cashless system, then, all types of fraud mentioned above are now electronic banking related frauds and there is need to discover the best way for detecting and perfecting of these menaces.

Chartered Institute of Management Accountants, (2009) differentiated frauds into several types which are also applicable to Nigeria economy. Frauds include the following: Frauds from any individual versus client; customers; consumers and others inform of misrepresentation of the quality of stocks or goods. Employee frauds versus employers

inform of payroll frauds; thefts of cash; falsifying expense claims; false accounting and thefts of assets.

In addition, frauds by the organisation or businesses versus consumers; investors and employees inform of falsification of financial statement; selling of fake goods as original ones; not paying tax. Frauds by the company or individual versus government in the form of grant frauds; tax evasion; and social security gain claim frauds. Frauds by professional criminals versus big companies in the form of mortgage frauds; advance fee frauds; money laundering; counterfeiting and corporate identity frauds. Electronic frauds by a group of individual or an organisation with the use of computers and information technology through the help of internet to perpetrate frauds inform of spamming; phishing; social engineering frauds; hacking; and copyright.

2.4 Impact of Fraud on Internal and External Stakeholders

E-banking fraud has become a global and provocative issue that produces debate among quite a few authors, for example Usman and Shah (2013), Tan and Rasiah (2011), Saleh (2013), Pandey (2010) and Oghenerukevbe (2008) stated that electronic banking fraud is a worldwide problem and is persistently too costly both to the banking sector and to customers. Until the mid-1990s, the banking industry in most parts of the globe was reliable and dependable (Dzomira, 2015). The new millennium started with an overabundance of activities that have contributed enormously to the academic field and the economy in general, especially electronic banking adoption by the financial institutions. Nevertheless, this e-banking adoption has become a global debate in the academic arena and the financial sector is not exempted (Barker et al., 2008).

Researchers in this phenomenon are still developing and formulating different theories for the electronic banking context (Mhamane & Lobo, 2012). Since the introduction of technology, the banking industry has experienced a paradigm change in the phenomenon (Dzomira, 2015a). However, with the development of technology, e-banking frauds have similarly increased.

Most statistical bases specify that e-fraud is on the increase, while local forms of fraud are usually in decline (Levi & Williams, 2013; Ablon et al., 2014). The Eurostat 2010 Information and Communication Technology survey undeniably confirmed that e-banking frauds have become the most rampant type of acquisitive fraud in both developed and underdeveloped economies (Anderson et al., 2012). However, the impacts of e-banking fraud were grouped into monetary and non-monetary impacts.

2.4.1 Monetary Impact of Fraud

E-banking fraud is a global phenomenon (Alao, 2016). Fraudulent activities have affected a lot of businesses in the banking sector (Rubasundram, 2015). The findings of the empirical study done by Anderson et al. (2012) offer details of e-fraud perpetrated across the globe in the banking sector, showing that globally, banks have lost billions of dollars to indirect and direct losses. Therefore, e-banking fraud losses continue to cause great problems for several industries, despite significant developments in fraud detection mechanisms. IIA, AICPA, and ACFE (2015), concurred that all electronic banking is susceptible to the menace of e-banking fraud. In reaction to the above, this is a time for the banking sector to give a zero tolerance for fraud; hence there is need for e-banking fraud detection and prevention.

Wilhem (2004) calculated annual losses through fraud for different industries in the United States of America to comprise $67 billion in insurance, $1.2 billion in banking, $150 billion in telecommunication, $40 billion in money laundering and $6.7 billion in e-banking. Also, the UK office of National Statistics reported in 2015 that the number of bank accounts being opened through fictitious or stolen identities had nearly doubled from the previous year, with over 23,600 instances reported in 2014 compared to 12,500 cases in 2015. This means, e-banking fraud is a universal problem.

Meanwhile, electronic banking fraud in the United Kingdom had increased from £40.9 million to £60.4 million. These losses occurred through the assistance of electronic transactions and are significant challenges to financial institutions in performing their role

in the economy (Office of National Statistics, 2015). In 2014, The German cybercrime watchdog, the Federal Office for Information Security, disclosed the stealing of 16 million email addresses and passwords (ENISA, 2014). Also, in 2014, three major world-wide e-banking frauds, together with the biggest ever documented, caused by the theft of customer records and counterfeiting of above two billion credit cards from large US retailers which caused liquidation of some banking industry and other were left in a state of insolvency (Perlroth & Gelles, 2014; Finkle & Hosenball, 2014). This indicates that, bankruptcy is one of the impacts of e-fraud and also, a lot of fraud incidences occurred are as a result of loss of customer's financial data or identity fraud

Generally, fraud activities eventually lead to bank failures. Financial Fraud Action UK (FFA UK) (2016) in their report between January to June 2016 Fraud Update: Payment Cards, Remote Banking and Cheque", reported £13.1 million loss in the United Kingdom to telephone banking frauds in the first half of 2016. In the third report of the European Central Bank of Nigeria (2014) on card fraud, the fraudulent transactions committed in 2012 within the "Single Euro Payments Area (SEPA)" totalled €1.33 billion, which serves as an increase of 14.8% from 2011. It was uncovered that 60% of the value of the reported fraud resulted from telephone and internet payments, 23% represented payment at point-of-sale (POS) terminals and fraudulent transactions, and 17% was from automated teller machines (ATMs). This shows that, all e-banking's channels of transactions are susceptible to frauds.

NIBSS (2015) that there was a significant increase of 78% in the volume of fraudulent incidents in 2014. The author's findings showed the vast amounts of ₦485, 194,350 (£1,239,690) and ₦6, 215,987,323 (£15,882,085) that were lost to fraudsters in 2013 and 2014 with 822 and 1461 cases respectively. NDIC (2016) reported ₦857 million (£2.2 million) actual loss sustained in electronic banking fraud in Nigeria, representing 27% of the total actual loss of the banking industry in 2016. Therefore, this confirms that, monetary loss is one of the significant impacts of e-banking fraud.

Moreover, regarding electronic payment system attacks, Financial Fraud Action UK (2015) reported that fraud losses on UK-issued cards in 2015 amounted to £567.5 million, an increase of 18% from £479 million in 2014. Saudi, Ismail and Tamil (2007), in their study titled "Phishing: Challenges and Issues in Malaysia", showed that in 2004 and 2005, the United States suffered losses of approximately $929 million from phishing frauds, the United Kingdom lost £12.2 million and £23.2 million in 2004 and 2005 respectively from phishing, and the loss suffered in Malaysia was RM18, 000 in 2003. Financial Fraud Action (2015) reported 1,028 cases of phone fraud in 2014 and vishing frauds costing £23.9 million in the United Kingdom in 2014, compared with £7 million reported in 2013. Apparently, vishing and phishing have negative impacts on the e-banking stakeholders.

US Payments Forum (2017) disclosed 16,594 victims and $517,653 loss to pharming attacks in 2015. Norse (2014), the Javelin study in USA, estimated losses over $4.9 billion from account takeover fraud in 2012. Meanwhile, Financial Fraud Action UK (FFA UK) (2016), in the report titled "Fraud the Facts 2016", reported actual loss of £29.4 million in UK financial industries through account takeover attack. Obviously, pharming and account impersonation are part of the major challenges facing e-banking activities.

In addition, Everyone API (2014), in the study "Fraud Mitigation and Identity Verification for Card Not Present Transactions" disclosed that businesses suffer losses of over $11,000,000,000 dollars yearly. The percentage of income lost to card-not-present fraud is increasing, rising from 0.51% in 2013 to 0.68% in 2014. Losses to merchants through phone, web, and mail order are mainly from card-not-present financial transactions. Likewise, Pandy (2016) declared in the study titled "Mitigating Fraud in the Card-Not-Present Environment" that card-not-present fraud resulted in 25% of global fraud losses and 45% of card loss in the US in 2015. And also, Dzomira (2015) study of "Cyber-banking Risk Mitigation" the Banking Industry in South Africa" reported R168.1 million and R189.2 million losses due to card-not-present fraud in 2014 and 2015. Therefore, there is a need to begin to develop strategies to mitigate card-not-present fraud, as several developing and developed nations have experienced significant spikes in this type of fraud.

Financial Fraud Action UK (FFA UK) (2016) reported a £39.24 million loss for skimming device fraud. According to RSA (2010), this increase is a result of an increase in usage of advanced and sophisticated tools by the fraudsters to target internet banking users through the automated pickpocket machine to pick card data and malware which targets vulnerabilities in the user's computer rather than the bank's own devices, which are hard to attack. Furthermore, the recent upsurge in fraud provides growing evidence that networks of malware and hijacked computers serves as most momentous threats in relation to present-day identity theft.

2.4.2 Non-Monetary Impacts

Manyika and Roxburgh (2011) argued that the banking sector and customers suffer not only money loss, but also non-monetary loss due to the incidence of frauds. Fraud has a negative impact on operating efficiencies, reliability of services, companies' reputations, investors' confidence, employee morale, and can also lead to potential fines levied by regulatory bodies (BITS, 2003). Unfortunately, electronic banking causes huge investment losses, substantial legal charges, loss of assurance in capital investment, and imprisonment of important individuals (IIA, AICPA & ACFE, 2015). In addition, Norse (2014) supported the view that electronic banking fraud can lead to loss of consumer trust, damage brand reputation, cause financial damages, and endanger compliance with financial institutions' regulations.

Generally, in conclusion, there is a need for the collective accord of regulators and banks to enact policies and implement measures to protect and prevent the banking system from e-fraud threats. Therefore, the importance of appraisal of electronic banking fraud prevention and detection cannot be overemphasised. Hence there is a need for incessant improvement in safety and security to avert frauds and alleviate the risks suffered by banks, customers and other industries, which have resulted in loss of confidence in electronic banking systems.

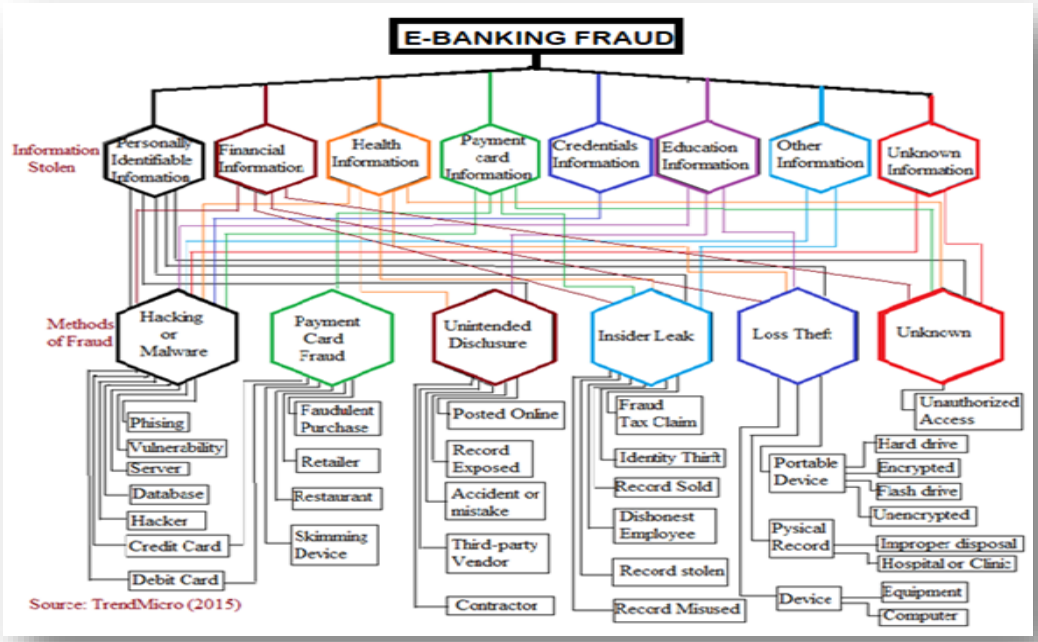
2.5 E-Banking Attacks and Techniques

There are several major information types targeted by e-fraudsters to defraud an individual or an organization: personal data, educational information, health information, credential information, payment card data, financial information, others and unknown through hacking or malware, insider leaks, payment cards, fraud loss or theft and unintended disclosures (see Figure 2.1).

Also, Park (2015), in a study titled “Follow the Data: Dissecting Breaches and Debunking Myth” supported the view that malware or hacking are employed to compromise any kind of records through phishing, unauthorized access to servers, vulnerability manipulation, compromising of databases and servers and unauthorized access to debit and credit cards. Restaurants and retailers were sufferers of payment card fraud through skimming devices, use of POS RAM scrapers of collecting payment card information, and frequent fraudulent transactions through stolen payment card data

Moreover, unintended disclosures occurred because of accidental posting of personal identification data, education data and health data online, and negligent data leakage by third parties and contractors. Insiders such as employees are also involved in fraud; they usually target financial information, personal identification data, and health and payment card data. They use these for fraudulent tax claims, to defraud customers’ accounts, for identity theft and for selling customers' data to outsiders with the aims of defrauding those customers’ accounts or committing other crimes. Loss and theft also compromise personal identification data, education data, health data, and financial data and make them vulnerable to fraud (Anderson et al., 2012). This happens through theft or loss of portable and removable devices (laptops, backup drives, USB keys and others); physical or hard copies of the records (bills, files, receipts and others); and stationary devices (office-use computers and other specialized business equipment).

Figure 2.1: Information Stolen and Methods of Fraud



In addition, Park (2015) stated that there are unknown methods that can cause online fraud incidents in banks, which can also compromise payment cards, financial data, personal identification information, education data and health data. The author's analysis across the industry between 2005 and 2015 in a Bayesian network showed that online fraud consisted of 25.0% malware or hacking, 24.0% portable device loss, 17.4% unintended disclosure, 12.0% insider leak, 11.6% physical loss, 5.4% stationary device loss, 1.4% payment card fraud and 3.2% unknown. Therefore, there is a need to take cognisance of the above to have effective prevention and detection of electronic banking fraud in financial institutions.

Additionally, the United Computer Emergency Readiness Team (US-CERT) (2015) supported the view that unauthorized access in the situation of electronic banking implies that an individual or group of individuals access a bank's or a customer's system without permission. This can result in the theft or loss of account information, personal

identification information and account passwords, and the transfer of vast amounts of money through the same system into an unknown account. Another method is when unauthorized software is installed in the victim's computer system, for example, malicious code, infecting systems with viruses, recording of keyboard strokes, and stolen data.

Moore, Clayton and Anderson (2009) concluded that there are various categories of attacks of electronic banking, but all may involve either stealing authentication identities from the victim or altering the victim's reasonable transactions. Moore and Clayton (2009), and Wang, Rashid and Chuang (2011) categorized attacks as a means of denying the victim access to their bank, or else watching their e-transactions. However, the aims and objectives of hackers are different. Hackers may decide to exploit vulnerabilities in targeted operating systems or gain unauthorized access to a website to deny customer services (Brar, Sharma & Khurmi, 2012). Attackers or hackers have several ways they use to gain access to the targeted system. However, the challenge facing information systems today is takeover within the system of computers and communication (Omariba, Moses, and Wanyembi, 2012). Therefore, information service providers and financial institutions need to guard against diverse types of electronic attacks to accomplish safe and sound communications in the networks of information systems.

Furthermore, researchers have categorized the diverse types of attacks against electronic banking in several ways. Vrincianu and Popa (2010) reported that the main types of attacks on the security of electronic banking are illegitimate use, denial of service, repudiation and disclosure of information. Dalton and Colombi (2006) suggested a hierarchy of causes which involved three main categories: credential theft, device compromise and illegitimate access. Peotta, Holtz, David, Deus and Sousa (2011) adopted an attack tree model to represent the major attacks and how they associate with each other; for example, phishing attacks, and social engineering, malware to gain control of system devices, and malware and fake web pages for credential theft from an authentic user.

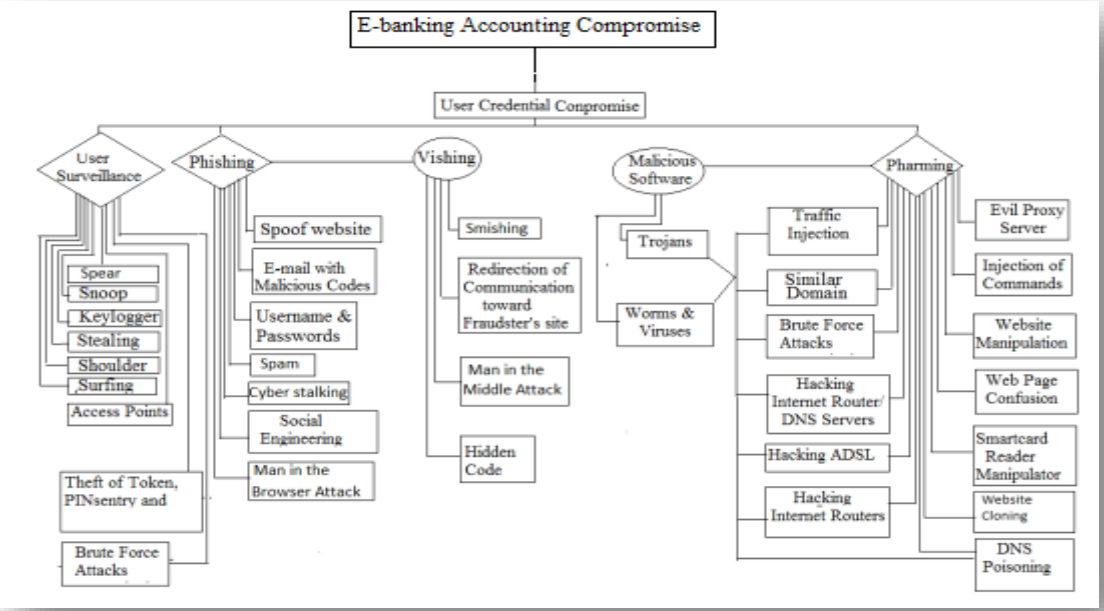
Omariba, Moses and Wanyembi (2012) classified the different attacks that electronic banking can suffer into the following types: port scanners, social engineering attacks, phishing, Trojans, pharming, denial of service, PIN hacking, super user exploits and server bugs. Conversely, Brar, Sharma and Khurmi (2012) grouped attacks into three major categories: local, remote and hybrid attacks. Local attacks occur on the user's device: when the bank website is opened, the uniform resource locator (URL) in the address bar is not spoofed, and the yellow secure sockets layer (SSL) padlock exposes the correct certificate information; but only an overlapped fake password prompt is maliciously set on.

One common type of local attack is shoulder surfing, which is usually related to observing and detecting the personal identification number for a bank card, before stealing the physical bank card either by pickpocketing or by force (Brar, Sharma & Khurmi, 2012). Remote attacks do not modify the user's device but aim to redirect or intercept the traffic of a session. Phishing, vishing and cloned voice-banking systems are some of the types of remote attacks (Brar, Sharma & Khurmi, 2012). Bo and Surya (2003), in a study of reputation services in electronic markets, stated that Trojans are programs that compromise a computer without the knowledge of the user. Lewis (2011) posited that the most globally documented malware in e-banking fraud is recognized as being the Zeus Trojan. Likewise, Bo and Surya (2003) also estimated that the Zeus Trojan was accounted for about 90% of the e-banking fraud across the globe since it had been placed into the financial market. Zeus has developed into almost a variety of forms of Trojan.

Finally, hybrid attacks are a combination of both local and remote attacks. A Trojan is the best example of a hybrid; it will be executed on the vulnerable system, examining all saved bookmarks and exchanging any useful online service URL with a counterfeit one (Omariba, Moses & Wanyembi, 2012). The Trojan also modifies the browser settings to disallow the address bar from displaying or overlap it with a forged pop-up window to prevent the user from seeing the modified URL (local attack). The more sophisticated the approach taken against an attacker, the more attackers also redirect domains and change

the host file to predefine the Internet Protocol address (Brar, Sharma and Khurmi, 2012) (see Figure 2.2).

Figure 2.2: E-Banking Account Compromise



However, the followings are the most common attacks used by the fraudsters to commit e-banking frauds. These are discussed below. First, electronic Payment System frauds: These are the manipulation of account information through electronic payment devices such as a debit or credit card for direct payment Hoang, Hu, Bertok (2003). However, Financial Fraud Action UK (2016) reported fraud losses through UK-issued cards in 2015 amounted to £567.5 million, an increase of 18% from £479 million in 2014. Correspondingly, KPMG (2016) KPMG Forensic Services report of investigation carried out on "Top Five Fraud Trends in Nigeria's Commercial Banks in 2016" shows that, Nigeria suffered actual loss valued ₦485, 194,350 and ₦ 6,215,987,323 of electronic payment frauds in 2013 and 2014 respectively.

Second, phishing is the fraudulent perpetration of sending electronic mail or pull-down (pop-up) web pages claiming to be from legitimate enterprises so as to convince people or entities to provide sensitive or personal account and business information such as

account information, credit card numbers, passwords and memorable words (Brar, Sharma and Khurmi, 2012). Phishing occurs when the fraudsters set up a fake copy which includes all the code of the web site targeted to impersonate on a server they control. Next, the fraudsters may send an email of convincing messages to the numerous number of email addresses, to deceive the recipient of the email and to mislead them into the spoofed web site by revealing their log in information Hoang, Hu, Bertok (2003).

Jakobsson (2005) opined that phishing is a popular method of stealing authentic identifications of the victims. Abu-Shanab and Matalqa (2015) described phishing as an attack premeditated to influence the victim to give away their electronic banking information to an unauthorized party. The followings are some of the phishing techniques used to steal the financial information and identification data of the electronic banking customers, which are Trojan, Shoulder surfing, Social engineering and key loggers (Symantec Security Response, 2005). Phishing web sites are the most popular attack form of credential stealing in the world, commonly joint with an email with deceptions to have access to the user's websites (Hooks, Kaplan, Schultz and Ponemon, 1994). Bossler, (2009) opined that phishing websites are totally a social engineering fraud which depend on the user's understanding of system security and problems with the way indicators of security are presented to the users. The attached model below describes in more detail the phishing attack.

Chaturvedi and Meen (2016) suggested that phishing attacks can be carried out through the following methods: Domain Spoofing, URL Modifying and Web Site layout similarities. Saudi, Ismail and Tamil (2007) in their study titled "Phishing: Challenges and Issues in Malaysia" shows that between 2004 and 2005, United States suffered losses approximately $929million from phishing frauds and United Kingdom lost £12.2 million and £23.2 million in 2004 and 2005 respectively through phishing on the web banking while, the loss suffered in Malaysia is RM18, 000 in 2003.

Third, vishing occurs when the hackers, phone the victims and trick them to reveal some secret data through the uses of social engineering. Cloned voices-banking systems happen as a result of many vishing attacks by clone the voice in the banking systems so that it

sounds similar as the original banking systems. Fake e-mail is adapted to beseech customers to call a number claiming to be their bank (Dalton, and Colombi, 2006). In the report of the Ombudsman (2015) titled "Calling Time on Telephone Fraud" describes vishing as voice phishing, as the fraudsters' practice of employing the phone to deceive and defraud people. Vishing is another means used by the fraudsters to gain access to victims' account information. The author termed vishing as "no hang-up fraud" which involves giving away of account information, personal identification number details and online money transfer over the phone. CIFAS, (2010) corroborate the issue in the report titled "Digital Thieves", text phishing and phone vishing frauds are increasing every day.

Action Fraud (2015) reported 1,028 cases of phone fraud in 2014 and vishing frauds of £23.9 million losses in the United Kingdom reported in 2014 compared with 7 million reported in 2013. Financial Fraud Action UK (FFA UK) (2016) in the report of "January to June 2016 fraud update: Payment cards, remote banking and cheque" reported £13.1 million loss in the United Kingdom to telephone banking frauds in the first half of 2016. This is done by the use of cloned voice-banking system, voice-over-IP and automated answering systems (Abu-Shanab & Matalqa, 2015).

Fourth, pharming is used for hijacking and stealing the web address of service supplier. This happens when a service user enters a Web address and it transmits to a Web site of fraudsters without the knowledge of the senders. The website will resemble the legitimate website with the intent of capturing confidential information of the sender (Kirda & Kruegel, 2014). Pharming refers to wrong direction of a criminal website through technological means. For example, an electronic banking user, who usually accesses his internet banking website, may be misdirected to an illegal website instead of being directed to his own banking website or legitimate website (Brar, Sharma & Khurmi, 2012).

Pharming is an illegal practice in which malicious software is installed on a user computer system or server, misleading the users to criminal websites without the consent of the users. Pharming can happen in four distinct ways: spoofing, malicious, hijacking and domain name server (DNS) poisoning (Abu-Shanab and Matalqa, 2015; Brar, Sharma

and Khurmi, 2012; Peotta, et al., 2011; Dalton, and Colombi, 2006). Spoofing occurs when the pharming criminal uses slight mistake in the domain name or fake domain name to divert the attention of the user from accessing the intended website to have unintended visiting into pharming criminal's website. For instance, a pharming criminal may redirect the user to www.mydmu.dmu.au.uk instead of www.my.dmu.ac.uk (Abu-Shanab and Matalqa, 2015). Likewise, malicious software (Malware) occurs through Trojans and viruses installed in a personal computer of the user by interrupting and diverting the user's attention to access the criminal website instead of the intended website (Peotta, et al. 2011).

Equally, domain hijacking is a situation when the hacker redirects transmits of the legitimate online traffic to an illegitimate website. This can be done in two ways: Domain slamming is an unauthorised transmission or a domain registration scam in which fraudulent domain name administrators tricks the domain holders to switch from original and legitimate registrar to their fraudulent domain registrar or illegitimate server (Abu-Shanab and Matalqa, 2015).

Correspondingly, domain expiration is a situation when a domain name is leased for a specific period and the lease agreement procedure is not properly managed until it resulted to wrongly transfer or loss of legitimate ownership (Dalton, and Colombi, 2006). This is usually occurs through mail of notification of expiration sent by fraudsters, not original domain registrar to legitimate domain service users notifying them that their domain registration services are about to expire and the mail contains the means of renewal or purchase engine traffic generator software which contradict to the original domain service or is the service the recipient of the main has never procured or used and probably does not want (Peotta, et al. 2011). Similarly, Domain Name Server (DNS) poisoning: This is a dangerous pharming which happen when a user enters domain name and the domain name server on the internet protocol address change the domain name and redirects the user to another website or fraudster's website. This poisoning can happen as a result of malicious software (Malware) installed on the server, misconfiguration and network vulnerabilities (Brar, Sharma and Khurmi, 2012). Respectively, Jackson (2009) explained

that, 13 root DNS servers are available for the entire internet, which are strictly control and protected. Utmost of the requests are directly transferred from the local DNS server into root DNS server. However, if hackers were to infiltrate any of these root DNS servers, the internet banking would be violently compromised. US Payment Forum (2016) disclosed 16,594 victims and $ 517,653 loss to pharming attack in 2015.

Six, Account takeover occurs when a person or a group of people overthrow another person's account, through capturing of the confidential information of the targeted victim, and then communicating the card issuers by impersonating the legitimate cardholder and requesting for a mail to be forwarded to a forged address. The fraudsters then report for loss of card and enquires for a reissued card to be sent. The fraudsters may then create a new PIN so as to free to use the card until the legitimate cardholder notices the deception when tries to use the card and discovered that the account has been drained (Hoang et al, 2003).

Account Takeover also called Facility Takeover. Fraud happens when a third party impersonates someone by making an application for insurance, credit or other services to hijack a person’s existing policies, accounts or other similar services and use them fraudulently (Sharma & Khurmi, 2012). Pandy, (2016) opined that account takeover occurs when a fraudster uses stolen identifications harvested from stolen documents, payment cards and data breaches to create new accounts.

Financial Fraud Action UK (FFA UK) (2016) explained that accounting takeover happens when a fraudster fraudulently uses another person’s debit or credit card account, first by collecting accounting and personal information about the targeted victim, then communicate their credit card issuer or bank to pretend as the legitimate card or account. The fraudsters then plan for funds to be paid out of the bank account, or they can change the legitimate address on the bank account and request for replacement or new cards to be sent which can be then used fraudulently.

However, Norse (2014) the Javelin study estimated losses over $4.9 billion from account takeover fraud 2012 which represent an increase of 69 percent in 2011$4.9 billion. While, Financial Fraud Action UK (FFA UK) (2016) in the report titled “FRAUD THE FACTS

2016" reported actual loss of £29.4 million in UK financial industries through account takeover attack.

Seven, Card-Not-Present fraud: An illegal use of card information on the internet or through the phone (Anderson et al., 2006). Pandey (2010) Card-not-present happens when payment made for a procurement using a debit card or a credit card at where the card is not physically present to permit the bank or card issuer to authenticate the cardholder at time of transaction or purchases, such as payments transaction made by phone internet or mail. For instance, EveryoneAPI, (2014) the findings of the study "fraud mitigation and identity verification for card not present transactions", disclosed that, businesses suffer losses of over $11,000,000,000 dollars yearly. The percentage of income lost to card-not-present fraud is increasing; rising from 0.51% to 0.68% in 2013 and 2014 respectively. Losses through phone, Web, mail order to merchants are mainly from card-not- present financial transactions. The author in 2012 concluded that 42% of Americans had been the victims of credit card fraud in the last 5 years. Likewise, Pandy (2016) declared in the study titled "Mitigating Fraud Risk in the Card-Not-Present Environment" that Card-Not-Present fraud resulted to 25 percent of global fraud losses and 45 percent of card loss in U.S. in 2015. Likewise, Chigada and Ngulube (2015) survey on card fraud, banking industry in South Africa" reported R168.1 and R189.2 million fraud losses due to card-not-present (CNP) in 2014 and 2015. Therefore, there is need to begin developing strategies to mitigate card-not-presented fraud as several developing and developed nations experienced significant spikes of Card-Not-Presented fraud.

Eight, skimming is a fraudulent practice by gathering of payment card information using electronic device. The smart card can be inserted in the point-of-sale (PoS) terminals or automated teller machine (ATM) that allows fraudsters to capture card details including cardholder's name, card numbers, issued and expired dates, secret code and PIN. The introduction of wireless system has made it possible for fraudster to greatly download stolen information without physically appearances at the terminals (Ford, 2011).

Financial Fraud Action UK (FFA UK) (2016) described skimming as skimming devices attached to the automated teller machine to capture the details from the card's magnetic

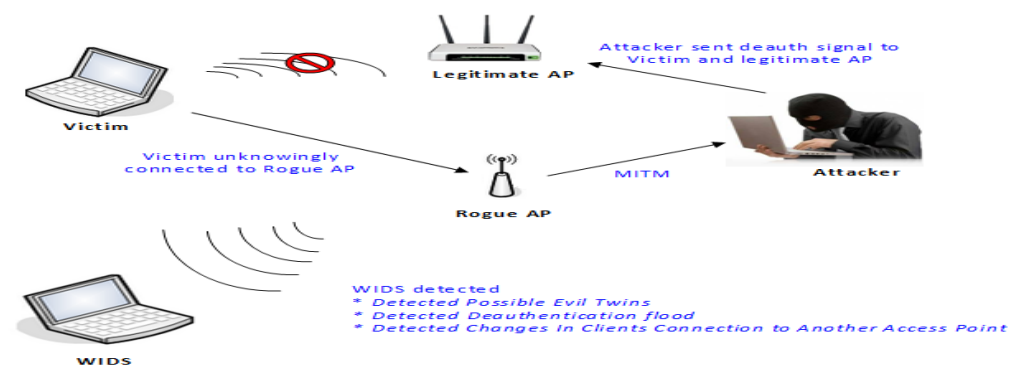
stripe while a miniature camera records the personal identification number (PIN) being entered FFA UK (2016).

A fabricated magnetic stripe card is then manufactured and used with the legitimate PIN to withdraw or transfer cash at machines within the country and overseas, which have yet to be advanced to PIN and Chip FFA UK (2016). While, Shoulder surfing is when the fraudsters watch the legitimate cardholder inserting and entering their PIN, then steal the card by using pick pocketing or distraction techniques. Financial Fraud Action UK (FFA UK) (2016) reported £39.24 loss to skimming device fraud. Chigada and Ngulube (2015) reported that banking industry in South Africa" disclosed R89.2 and R48.5 million fraud losses due to credit card skimming in 2014 and 2015

Ninth, SIM Swap fraud happens when the phone number of a bank customer is stolen through fraudulent SIM replacement at a Telco outlet/agent. The perpetrator then uses the mobile line to access the account of the victim usually via mobile banking or receives account sensitive details like PIN through PIN reset request (Bahnsen et al., 2013).

Tenthly, traffic injection is a traditional method of attack which uses to modify the financial transactions being made by the user so as to redirect it or vary the amount concerned. Traffic injection is done by manipulating and hacking internet router which the traffic passes or counterfeiting packets. Traffic injection can be done through evil tor nodes, access points, proxy server, hacking internet routers, Trojans and ADSL routers (Brar, Sharma & khurmi, 2012) (see Figure 2.3).

Figure 2.3 Traffic Injection



Park (2015) opined that injection aids, electronic fraudsters to steal electronic banking users' credentials and to inject and manipulate transactions while bypassing or evading two factor authentications. Since many banks use two factor authentication techniques (Sign In – Phone Banking Code and Sign In – Token) for transactions such as token and mobile phones, any unpredicted transaction notice will suddenly ring an alarm to the internet banking customers. This inject deploys a social engineering method when injecting a transaction.

2.6 The Contributing Factors for E-Banking Fraud Increase

With the global use of progressively advanced internet technology, electronic banking is developing as a great medium or network for banking businesses (Chanson & Cheung, 2001). However, electronic banking fraud perpetrations are becoming more sophisticated, unbearable, greatly intimidating the security and trust of electronic banking activities. Agwu, (2012) viewed electronic banking fraud as an epidemic disease in the banking industry, which has become a great challenge to both management and customers of the

industry. E-banking fraud has become a global and provocative issue that produces debate amid quite a few authors like Saleh, (2011); Pandey, (2010) that electronic banking fraud is a worldwide problem and is persistent to be overpriced to both banking sectors and customers.

Corroborating the views, Usman and Shah, (2013) frauds in electronic banking services happen as a product of several concessions in security extending from inadequate internal controls to feeble substantiation systems. Electronic banking fraud is now a thoughtful matter of financial crime management in all financial institutions. The development and advancement of challenging of electronic banking frauds such as ghost website, phishing scams and malware have coursed a massive loss in the banking industries worldwide (Wei, et al. 2013). Therefore, there is need to examine the causes of electronic banking frauds. Uchenna and Agbo (2013) a lot of factors contribute to the menace of fraud perpetration in Nigeria, which is grouped into: technological challenges and non-technological challenges. Ojo (2008) and Idowu (2009) also classified the causes of fraud in the banking industries into: the endogenous (institutional) challenges and the exogenous (environmental) challenges. Hence, for the benefit of this study, the factors contribute to the increase of e-banking fraud were grouped into technological factors and non-technological factors which explained below.

2.6.1 Technological Factors

The introduction of Electronic banking has come with its risks and challenges, starting from electronic banking adoption to financial transaction with the new system (Usman & Shah, 2013). The research concluded to several factors that impact the adoption and implementation process of electronic banking such as system security, accessibility, trust and social influence, the cost and time factors embedded in fund transfer, its usefulness and ease of use (Abu-Shanab, Pearson and Setterstrom, 2019). Security is a factor that is frequently emphasized as a critical success factor (CSF) for the success and effectiveness of electronic banking. The deficiency of security will possibly lead to negative media

publicity, financial losses and disciplinary measures by regulators. Security was ranked by some researchers as the significant concern of electronic banking operations (Yan et al, 2009).

Moreover, grounded in an empirical analysis completed on real world transaction datasets, Kovach and Ruggiero, (2011) discovered that a lot of electronic banking accounts were defrauded by only one fraudster, which involved a small amount of money transaction with a total amount of money larger than one account. The author concluded that many frauds occur as a result of increased number of password failures which give opportunities to fraudulent behaviours. Correspondingly, in the survey carried out in Australian banks on electronic banking frauds, the finding showed that almost electronic banking frauds have the following challenges and characteristics, ineffective real time detection, weak forensic evidence, dynamic fraud behaviour, imbalance large datasets and diverse behaviour patterns of customers (Wei, Cao, Ou, & Chen, 2012).

Jassal and Sehgal, (2013) in their study titled "electronic banking security flaws" aimed at finding diverse types of faults in the security of electronic banking that end to loss of money by customers and banks. The authors discussed the reasons of security breaches and the involvement of both banks and customers in giving a chance to crackers and fraudsters to have access into their networks through web-browser installed on their customer's personal computer which give opportunities to unauthorized persons to have access to their personal identification information and financial information (Nor, Shannab & Pearson, 2008). Usman and Shah, (2013) viewed electronic banking fraud as a global issue which is persistent to prove costly to both banking sector and its stakeholders. Electronic banking frauds happen because of different concessions in security started from feeble authentication systems with inadequate internal controls.

Electronic banking fraud could be from bank website, such as cross site scripting through malicious and SQL statement entered by attackers into the web page of the bank (Schneier, 2011). Omar et al. (2011), argued that most stakeholders willing to use electronic banking services because of its convenience, cost effectiveness, speed and easy accessibility, but the finding reveals that ATM machine problems; electronic frauds and

insecurity. European Central Bank (2014) reported that card fraud payment is one of the major means of fraud such as counterfeit card, card not received, lost and stolen cards. The author further elucidated that the contemporary mobile devices with their operating system were not intentionally produced with the security of financial payment, the transmission of personal data and sensitive payment through the use of radio technology leaks mobile payment to risks, unlike traditional payments, mobile payments expose include extra actor in the signal transmission such as mobile network operators and also, the general public may not have adequate awareness of the associated information security risks attach to use of mobile devices and internet desktops or laptop for payment at home.

Correspondingly, Adedipe (2016) in the study internet fraud, findings show that, the external fraud is fundamentally direct outcome of hackers' activities which include unauthorized access to electronic bank account information which are accomplished through pharming attacks, phishing attacks, session hijack, skimming attack, eavesdropping hijack, brute force attacks. These are emanated through bank staff and customers' ignorance and unawareness of common social engineering techniques, negligence in displaying PIN code and accounting information, and carelessness disposal of computer devices and related software.

Deloitte (2015) in the study of "India Banking Fraud Survey" discovered that there is increase in the electronic fraud occurrence in the banking sector because of lack of the tools and technology to discover the potential red flags. Likewise, Regha (2015) concord that difficulties in preventing electronic banking frauds could be influence by the following factors which involve: ineffective monitoring of electronic banking channels such as ATM terminals, internet banking, telephone banking, personal computer banking and card teller banking, non-existence of camera such as CCTV at e-banking transaction terminals, absence or inadequate of system base solution to trace and to report suspicious transactions and compromised accounts, lack of compliance to Know-your-customer and best practice procedures of e-banking management, no segregation of transaction limits, failure of incorporating string validation test of security, ineffective encryption key

management, inadequate control to restricted environment and availability of ex-staff with active login pin to e-banking management system data base.

Equally, Odediran (2014) the findings in the study titled “holistic approach to electronic channels fraud management” shown that, the factors that influence the rising cases of electronic banking frauds in Nigeria are Ignorance of cardholders on card usage security, Inadequate monitoring of electronic payment terminals and lack of adequate management of electronic bank production services. Gates and Jacob (2009) have pointed that the factor contributes to increase of e-banking fraud is the mismanagement of technology in the banking industry which comprises use of technology for illegal activities, sharing of confidential data, banking access for over-payments to sellers. European Central Bank (2014) in the survey of cards fraud, further elucidated that the contemporary mobile devices with their operating system were not intentionally produced with the security of financial payment, the transmission of personal data and sensitive payment using radio technology leaks mobile payment to risks. Banking services and other financial industries experience losses annually through fraud incidences such as internet banking frauds, cheques and cards frauds (Adams, 2010). Therefore, these obviously signify that fraudsters are exploiting electronic banking channels.

Moreover, Brunner et al. (2004) in their survey, found that the location of Automated Teller Machine (ATM) is a high determining factor for fraud perpetrating at Automated Telle Machine point. From this study, above 75% of the respondents confirmed that the location of Automated Teller Machine (ATM) in isolated places without surveillance security such as Closed-circuit television (CCTV) , Video Surveillance and Security officer subsidise to the fraud occurrence at ATM point. Therefore, Automated Teller Machine (ATM) within the premises banks is more secured and, it is noticeable that the location of Automated Teller Machine in attractive environment or location does not support it prone for fraud.

Correspondingly, Diebold (2002) reported that the significant form of Automated Teller Machine(ATM) fraud is personal identification number or information (PIN) theft which is performed through several means; shoulder surfing, skimming, camera, key pad recorder and other related means. This study explicates that the major type of perpetrating fraud during the Automated Teller Machine(ATM) is PIN theft which is commonly happening when there is overcrowding of the users at Automated Teller Machine points. In the same vein, in the investigations of Bernett (2000), and Oko and Oruh (2012) found that 24 hours' access to the Automated Teller Machine or point of sales (POS) devices is a "double edge sword" it has both disadvantage and advantage.

Therefore, it is easy to construe that automated teller machine (ATM) fraud incidents occurred most in the day time. Also, no dispute, there are some incidences of fraud at night, but most automated teller machine users usually make transactions in the day hence, preventing fraud incidences at night paramount. In addition, Bernett (2000) reported that some banks have no provision for reporting of fraud incidences and there is no enough orientation for the customers on how to operate e-banking devices such as automated teller machine, POS and the similar, neither provision of Fair and Accurate Credits Transactions Act (FACTA) or Automated Teller Machine Manuals for the ATM users.

This also corroborated with Roberds, (1998) discovered from historical lesson learnt where insufficient security measures caused fraud in retail payment systems. This was backed up by example of cloning that led to losses of almost $600 million from the store's value card encryption. Hence there is need for incessant improvement in safety and security to avert frauds and alleviate the risks suffered by banks, customers and other industries which have resulted to lose of confidence in electronic banking systems (Giles, 2010). Moreover, presently some enhancement development in preventing fraud of electronic banking channels have been experienced. Financial Fraud Action (2011) testified to the actual fraud losses of 10% on credit/debit cards and 24% fraud losses on internet banking lower than the previous years in the UK. This has been accredited to

growth and development of electronic banking safety by the use of non-technical and technical approaches. Globally, to protect and safeguard electronic bank accounts and other financial information on their websites, banks spend substantial technology resources in terms of hardware, software, licensing fees, consulting fees and personal hours on providing an infrastructure that will protect electronic banking from fraudsters (FFA UK, 2016).

Moreover, technological factors, universally, the costs of managing e-banking fraud risk and the number of electronic banking fraud incidents are always increasing due to the sophisticated techniques used by electronic banking criminals (CIFAS, 2009). Symantec Security Respons (2005) found that internationally, on average, 116 e-fraud attacks occurred each day in 2012 through social engineering and customized malware, obtaining unauthorized contact with sensitive information, as against 82 attacks per day in 2011. Likewise, Avinash Ingole and Thool (2013) agreed that, phishing, card skimming, Trojans, spyware and adware, website cloning, cyber stalking, lack of sophisticated antivirus software and weak passwords contribute to the rapid increase of electronic banking fraud. Therefore, the importance of examination of electronic banking fraud prevention and detection cannot be over emphasised, hence this study.

2.6.2 Non-Technological Factor

Regardless of religion, ethnicity, culture and other factors, there are individuals that are still being motivated to perpetrate electronic frauds. Irrespective of technology, The American Institute of Certified Public Accountants (AICPA), and the Association of Certified Fraud Examination (ACFE), (2015) found that the financial pressure to make means is paramount to some individuals, opportunity and rationalization which are the main reasons why fraud happens. In the authors' research found that, 72 percent seek for personal gain while other 40 percent do not recognise their fraudulent actions as a motive for illegal behaviour.

Usman and Shah (2013) discovered that inadequate staff education, customer education and internal control are other areas which need to be addressed to minimise electronic

banking fraud. Grounded on an empirical analysis completed on real world transaction datasets. Dynamic fraud behaviour, fraudsters constantly advance in the techniques to overthrow electronic banking protection. Imbalanced large datasets, huge amount of money and time spend on electronic banking fraudulent transactions per day still, the process of detecting frauds becomes a difficult challenge (Wei, et al 2012). Lastly, diverse behaviour patterns of customers, electronic banking customers perform different transactions in diverse ways for various purposes. This is a challenge as it results to variety of genuine customer transactions that would be imitated by fraudsters who change their behaviour regularly to contend with advances in fraud detection, thus makes it hard to characterize fraud behaviour from genuine behaviour. BIS, (2012) viewed the cause of electronic banking fraud beyond electronics. The finding of these authors indicates that exploited staffs, lack of training, low compliance level and competition are the major reasons for electronic banking frauds. Therefore, there is need for banks to observe the rising graph of electronic banking frauds seriously and make sure that there is no slackness in internal control mechanism.

In conjunction with the above, Choplin and Stark, (2013) in an investigation conducted, the finding was that, the banking customers are vulnerable to electronic banking frauds both lack of education and demographics have impacts on consumers' vulnerability. Abou-Robieh, (2005) reaffirmed this, to prevent payment card fraud, consumer education on personal information protection is essential. Zimucha, et al (2012); Masocha, Chiliya and Zindiya, (2011) discovered that the causes of electronic banking frauds are insecurity, limited internet access, cultural barriers and poor legislation. While, Agboola and Salawu (2008) concurred with this, security is paramount issue of the effectiveness of electronic banking services. El-Guindy (2008) asserted that most banks are investing on development of electronic banking, but not on its security. Although Nigeria financial institutions have invested a lot on information technology infrastructures, most banks and e-businesses in Nigerian still lack cognizance of the significant of security in electronic banking. Therefore, there is a need to examine electronic banking frauds prevention and detection in more detail.

Roberds, (1998) ascertained that, opportunities or motives for electronic banking frauds rise in the situations when there is a transaction of enormous amounts, when there is unidentified transacted and, in a situation, when the parts to claim the payment suffer the cost of fraudulent transactions, thus the need for effective electronic fraud prevention and detection. CBN Annual Report, (2010) disclosed that, almost of electronic banking frauds occurred in 2010 are because of an inadequate internal control system. Odediran (2014) believed that, the internal fraud which is often committed by bank staff comprises mailing of wrong financial information, card and PIN code hacking, account records suppression and collusion with external fraudsters as a result of inadequate internal control and management oversight.

While, Sullivan, (2014) argued that, financial institutions bear huge losses yearly through electronic frauds such as card fraud, Automated Teller Machine frauds, misused of private passwords and negligent of the customers to their private transaction data. This signifies that fraudsters are taking advantages of electronic banking system. Then there is a need for substantial strategies for prevention and detection of fraud.

Kinkela and Harris (2014), in other hand, committing of fraud involve team-up of bank staffs with the security agents in both national and international networking. Surprisingly, the outcome of above author's research work revealed that internal staffs that have direct access to the records and personal data of stakeholders and the system of the bank are teaming-up with the fraudsters. Thus, standard procedures of recruitment and adequate training of the staff will contribute enormously in the prevention and detection of electronic banking frauds. Nkemdilio, Bonaventure and Kingsley, (2013) discovered that perceived job insecurity and inequality had great contribution to employees' fraudulent intent. This is consistent with one of the elements "perceived pressure" in the Fraud Triangle Theory. Therefore, this finding proves beyond technology, it means their other causes that could lead to electronic banking fraud; hence there is need for detection and prevention strategies. In other hands, another critical success factor is organisational learning in the framework of fraud vulnerabilities from the perspective of historical lessons learnt.

Furthermore, Ganesan and Vivekanandan, (2009) warned that the manner of opening an internet account on the internet and transaction security on the internet must be paramount to both internet bank account holders and the bank managements. This also corroborated by Roberds, (1998) discovered from historical lesson learnt where insufficient security measures caused fraud in retail payment systems. This was backed up by example of cloning that led to losses of almost $600 million from the store's value card encryption. Chartered Institute of Management Accountants (2008) showed lighter to the occurrence of electronic banking fraud that electronic banking frauds occur because of need or greed. The author buttresses the point that 63% of fraud cases cited in 2007 were as a result of greed or people's needs. Other causes are challenges from gambling and debts.

CIMA (2008) opined, Temperament and personality also play a vital role in the occurrence of fraud. Some good people with good aims and agenda or principles can equally find themselves in the bad company and beginning to have a taste for the quick and fast better life, which lures them to the fraud. Chartered Institute of Management Accountants, (2008) looks at the perspective of pressure or motivation which is one of the elements of Cressey in the Fraud Triangle. KPMG (2006) concluded that, fraud is certain to occur in an organisation where there is a feeble internal control system, possibility of detection and slight panic of exposure, uncertain policies regarding satisfactory behaviour.

These authors are in support with the opportunity as an element of fraud triangle theory as also, research has revealed that some workers are completely honest, some are completely dishonest, but there are many that are influenced by opportunity. In corroborate with above, CIMA (2008) and KPMG, (20006) agreed that fraud can still be committed through the concept of reasoning of some people, some people may perceive fraud that is necessary to be committed particularly when done for business, when some perceive fraud that is harmless because the affected organisation or victim is big enough to mesmerize the impact and also many people may see perpetrating certain fraud that is justified because the organisation or victim deserved it or because those perpetrators have already been mistreated by the company's management or company. From the above,

these researchers argued that rationalisation as one of the elements of the fraud triangle is also a vital cause of fraud, even without respecting the nature or kind of the fraud either electronic banking fraud or non- electronic banking frauds. Therefore, to commit any fraud, especially, electronic frauds there must be an element of rationalisation in the mind of the perpetrators.

Shah, Brayanza and Morabito (2007) believed that, incompetency and lack of knowledge of the customers have caused losses and the failure of some banks and customers. Therefore, there is a need to teach customers the cause and prevention of electronic banking. Chartered Institute of Marketing (2008) posted that the causes of electronic banking frauds associated with human perspectives which have to do with motivation of the prospective fraud perpetrators, the conditions of rationalise the prospective fraud, opportunities to perpetrate frauds, perceived appropriateness for the targeted fraud, technical ability and capability of the perpetrators, expected risk of discovery after the fraud has been committed, expectations and actual consequences of discovery.

The AICPA and ACFE (2015), the ineffectiveness of online security results to electronic banking frauds, financial losses as well as a result of inadequate disciplinary measures by regulatory body, lack of customer due diligence which means failure to identify beneficial account owners and company owner and also, other professionals such as accountants, lawyers, police and estate agency fail to play their roles when a fraudster set up unidentified company to hide behind, purchase property, this transaction usually needs the services of these professionals. As electronic banking frauds are influential issues to the word security and desire to be meticulously controlled.

Deloitte (2015) in the study of "India Banking Fraud Survey" observed that there is high frequency of electronic fraud occurrence in the banking industry because of absent of oversight by the top management on movement from the present programme, pressure from business to meet unreasonable target and collusion between the external parties and internal parties (employees). The above authors concluded that, the most challenging issues of fraud increase, are inadequate customers and staff awareness, unable to integrate data from different sources and lack of research in this field, hence this study to assist in

maintaining security and protecting stakeholders from sustaining loss and losing confidence in electronic banking.

Furthermore, the endogenous factors are other factors to consider which also known as the institutional factors, are those factors that can be traced to the internal environment of the banking industry. The endogenous factors are feeble internal control and accounting system, weak customers relation procedure, pay no attention to know your customers rule, ineffective information technology system management, poor management of data base system, poor condition of service and salaries, frustrations from personnel strategies and policies, lack of incentive and promotion, unfulfilled promises by the management, irregular call-over, failure to report fraud incident, insufficient infrastructure, poor generic traits and scanty training, Staff enrolment centred on sentiments, and lack of constant re-training (Ojo, 2008; Adeyemo, 2012;Uchenna and agbo, 2013).

Usman and Shah (2013) stated that frauds in electronic banking services happen as a product of several concessions in security, extending from inadequate internal controls to feeble substantiation systems. Hence there is a need for appraising the factors contributing to the increase in e-banking fraud. Also, the CBN Annual Report of 2010 disclosed that almost all the electronic banking frauds that occurred in that year were the result of inadequate internal control systems.

Equally, Calderon and Green (1994) examined 114 actual incidences of corporate frauds issued by the Internal Auditors between 1986 and 1990. The authors concluded that improper segregation of duties, lack of proper records, and poor internal controls were responsible for almost all fraud incidences. Correspondingly, Jeffords, Marchant and Bridendall (1992) investigated 910 incidences presented by the Internal Auditors between 1981 and 1989 to appraise the exact fraud issues quoted in the Tredway Commission Report. Almost 63% of the 910 incidences were categorized as internal control frauds.

In addition, customers-staff collusion, according to Kinkela and Harris (2014), committing of fraud involves team-up of bank staff with security agents in both national and international networking. Surprisingly, the above authors' research work revealed

that internal staff who have direct access to the records and personal data of stakeholders and the systems of the bank are teaming up with fraudsters.

Deloitte, in the study "India Banking Fraud Survey" (2015) observed that there is a high frequency of online fraud occurrence in the banking industry because of the lack of staff integrity which gives chance to pressure from business and personal to meet unreasonable targets and collusion between the external parties and internal parties (employees). Additionally, the study of Usman and Shah (2013) "Internet Banking security" disclosed that 45% of the fraud incidences reported in 2012 included the involvement of managerial and professional staff.

Additionally, ineffective procedure of fraud reporting, AusCERT (2006), in a survey of Australian Computer Crime and Security (ACCS), concluded that the respondents from the organizations that had experience of electronic banking fraud had agreed not to report fraud incidents to anybody outside of their organization as this would cause damage to the company reputation, did not really know the impacts and capabilities of law enforcement agencies, and believed that if all the frauds were reported the fraudsters would not be caught as a result of lack of regulations and records (AusCERT, 2006).

Besides, negative impressions of bank stakeholders to law enforcement agency, Muscat et al., (2002)**,** this shows that organizations have different negative impressions to law enforcement agencies and this challenge creates a chance for fraud occurrence; there is thus a call for prosecution as a tool for fraud prevention as positioned by fraud management lifecycle theory and as guardianship in routine activity theory. Correspondingly, individual customers may choose not to report the maltreatment they suffer from fraudsters for certain reasons such as unawareness of the impacts of law enforcement agencies and a feeling of taking responsibility for all loses involved (Yar, 2005)**.**

Similarly, Zimucha et al. (2012) and Masocha, Chiliya and Zindiya (2011) discovered that the causes of electronic banking frauds are insecurity, limited internet access, cultural barriers and poor legislation. The study of El-Guindy (2008) supported the view that most banks are investing in the development of electronic banking, but not in its security.

Sullivan (2014) argued that financial institutions suffer huge losses yearly through online frauds such as card fraud, automated teller machine frauds, misuse of private passwords and negligence of customers of their private transaction data. This signifies that fraudsters are taking advantage of the electronic banking system. Thus, there is a need for substantial strategies for prevention and detection of fraud.

Dorminey et al. (2010) stated in line with Donald Cressey1953, that the fraud perpetrators use their position of trust to find an illegal solution to a monetary challenge and believe that nobody will see them, or they are unlikely to be caught, this is known as perceived opportunity. Lister (2007) elucidated opportunity as the "fuel that keeps the fire going", which means that however high the degree of motivation, a fraud perpetrator cannot commit fraud without having the opportunity. Taylor (2011) supported this view with examples of opportunities such as poor management of turnover, improper segregation of duties, and ineffective organizational structure. Soltani (2013) consented that position is an opportunity for someone who is a fraudster or trust violator to commit fraud. He also opined that there is a link between power to conceal fraud and opportunity to commit fraud.

Wolfe and Hermanson (2004) described opportunity as a weakness in the internal control of an organization which allows employees to commit fraud. Albrecht, Albrecht and Albrecht (2008) mentioned the lack of audit trail, ineffectiveness of internal controls, weakness of the board of directors, lack of effective anti-fraud disciplinary policy, and other factors as perceived opportunities to commit fraud. Tessier (2013) agreed with the rationalization that almost all trust violators see themselves as honest people who are found in a bad position. This enables them to assess the crime as an acceptable thing to do for them. Authors have explained further that many fraudsters have the idea that what they are doing is illegal or completely wrong at that moment, but they just deceive themselves by thinking that it is ilegal. Rae and Subramaniam (2008) also opined that rationalization is an act of justification of trust violation because of lack of integrity or immoral thought in the lives of employees.

Albrecht, Albrecht and Albrecht (2008) used examples to describe the rationalization by which some organizations' managers or executives violate the rules and standards of financial statements by increasing the stock price arbitrarily or doctoring financial statements to favour their personal interest and still believe that it is for the benefit of the company. Given the nature of the Nigerian economy in relation to fraudulent incidents and lawless attitudes, this theory is most useful for discussing the causes of banking frauds in Nigeria. However, the fraud triangle theory is an inadequate model for detecting e-banking fraud. As is said by critics, the rationalization and pressure cannot be observed; also, it is not technologically oriented and is focused solely on the perpetrator.

Kassem and Higson (2012) argued that the factors of e-banking fraud increase have direct relationships with individual capacity and personality traits. As Soltani (2014) clarified, opportunity gives way to incentive or pressure for fraud, while rationalization leads trust violators to perpetrate fraud; but the fraud perpetrator must have the capacity – good knowledge of the internet and information technology – to identify opportunity and be able to exploit it to commit fraud. Additionally, Dorminey et al. (2012) list the crucial traits that need to be considered for committing fraud, particularly in a large organization: a person's position or function with the combination of ego, intelligence, and ability to handle stress may influence them with the capability to exploit or create an opportunity for fraud. Therefore, potential fraudster who is the position of authority in the organisation and knowledge the weaknesses of internal controls and able to take advantage of them through his position, authority and function.

Wolfe and Hermanson (2004) concurred that the largest frauds are committed by highly intelligent, creative and experienced people with strong power over the company's controls and management, and with sound knowledge of the company's vulnerability analyses and assessments. Kassem and Higson (2012) conceded that committing fraud and handling the fraud for a lengthy period is stressful. Therefore, a successful e-banking fraudster are the people in the elevated position in the organisation who has confident, perfect and effective in dealing with the internet, hacking information, and stress; and be in a position of authority to perpetrate frauds.

However exogenous factors are the factors within the external environment of the organisation which are job insecurity, family pressure, group pressure, societal expectations, individual financial burden, individual greediness, national economic recession, poor leadership culture, lack of security, inadequate infrastructure amenities and political instability. In the study of Regha (2015) concluded that ignorance of electronic banking and unawareness of tricks of fraudsters, many electronic banking customers have fallen into victims of the fraudsters. CIMA (2008) and KPMG (2006) found that the ineffectiveness of online security results in electronic banking fraud. Monetary losses occur as well as a result of inadequate disciplinary measures by regulatory bodies; lack of customer due diligence (which means failure to identify beneficial account owners and company owners); and other professionals such as accountants, lawyers, police and estate agencies failing to play their roles when a fraudster sets up an unidentified company to hide behind to purchase property (such transactions usually need the services of these professionals). Bhasin (2016) argued that frauds commonly occur in the banking industry when procedural and safeguards controls are insufficient, thus allowing the system to become vulnerable to the fraudsters or perpetrators.

2.7 E-Banking Fraud Detection and Prevention Mechanisms

It is universally accepted that banking industries cannot absolutely escape from the menace of fraud (Subramanian, 2014). There are always some people who are motivated to violate the rules or commit fraud, and an available opportunity can make people in an organization perpetrate fraud (MacGibbon, 2005). Therefore, there should be standard, adequate and flexible detection and prevention techniques which will be continuously changing to meet up with diverse changing fraud risks. Therefore, this section discusses the currently available detection and prevention mechanisms. They are discuss as following. First, internal control mechanism, Bhasin (2016) has described, Sarbanes-Oxley dictates that enterprises are strictly devoted to internal controls. However, the most systematic Sarbanes-Oxley compliance strength cannot offer complete security against

the occurrence of fraud. Proactive establishments will add extra controls, as well as thorough approval of segregation of duties and procedures.

Second, education, awareness and training mechanism, Bhasin (2016) in a study titled "Combatting Bank Frauds by Integration of Technology" stated that employees must understand the impact of the menace of fraud in the business. The employees need to identify the impact of deceptive behaviour and where and how to document it. Furthermore, treasury officers need to be properly trained and legally informed on how to use the enterprise's fraud protection technologies and tools. Third, Bank Verification Mechanism, Bhasin (2016), George and Jacob (2015) stated that one of the most significant insecurity problems organizations encounter is fraud committed by dependable insiders and customers. Human resources department and cash control unity must perform background verifications on prospective employees and customers, and honest testing is required from the organization itself.

Fourth, rules and Regulations Mechanism, Wells (2005), in the study "New Approaches to Fraud Deterrence", found that fraud risk management policies and procedures are appropriate and significant for prevention, fraud detection and investigation, and there is a need for reporting policies, resolutions and procedures to be communicated to organizations' employees. The author further suggested regulatory compliance, so as to ensure that suitable procedures and policies relating to company obligations for applicable and ethical conduct are in place, and to familiarize staff with the company's standards and criteria for ethical conduct. Bhasin (2016) stated that many establishments fire the staff that perpetrate fraud but circumvent prosecuting them for fear of spoiling the company's image. A zero-tolerance policy plays a significant role in minimizing the menace of fraudulent incidences. Similarly, company management should instantaneously take evidence or proof of suspected fraud to the law enforcement agencies.

Fifth, technological mechanism, there are various technological mechanisms used to prevent and detect e-banking frauds. Bhasin (2016), in a study titled "Combatting Bank Frauds by Integration of Technology", conducted via a questionnaire-based survey with 345 bank staff in Malaysia, listed the current tools for detecting e-banking fraud, such as automated analysis tools, data visualization tools, behavioural analysis, deep learning and internal audit functions. Bhasin (2015), in an investigation into the "Menace of Frauds in the Indian Banking Industry", found that the innovative detection and prevention technology employed by some banks, including Data Glyphs, Two-Dimensional Barcodes, Biometrics, Cheque Image Processing, Data Analytics and Data Mining, contributed to addressing the problems of fraud detection and prevention. Therefore, banks need to discover and implement an appropriate sophisticated technique against fraud incidences.

Avinashingole and Thool (2013) posited that banks have different incentives and technologies for preventing and detecting frauds in e-banking services. However, it is mandatory for every banking industry to have adequate rates of incentive and technology to protect customers from the menace of card payment fraud, compromised accounts, and identity doubtful. George and Jacob (2015) presented a risk scoring model as one of the best prevention tools. This model is centred on the current statistical data on card holders, related with the historical data. The outdated method of authenticating via passwords and usernames is not going to be functional and effective in the contemporary system, which needs the support of unconventional technology. Therefore, George and Jacob (2015) concluded that electronic banking fraud prevention and control should be focused on fraud prevention software, smart card authentication, one-time passwords and biometric authentication. The authors further testified that biometric technology provides a better authentication technique and improves security.

In the present day, in the banking sector, several technologies have been adopted to fight fraudulent activities, for example one-time passwords (OTPs). This is an indispensable technique, involving the display of a time-determine code which an e-banking customer needs to insert into the payment or deposit devices of the banking system (Johnson, 2008).

USB Tokens, PINsentry, cards and smart cards are other security instruments used by banks to verify e-banking customers through their custody of any of these security devices. The challenge is that all these current security instruments cause one problem or another. For instance, USB tokens initially need another hardware device and cannot serve its purpose if access is restricted or the available computer has no USB ports (Council FFIE, 2011; Longo & Stapleton, 2002).

Sixth, transaction monitoring is another technique that has been formed for a variation of bank card fraud deterrence approaches. This technique investigates the receiver and sender of a transaction, compared with previous acknowledged fraud incidents. Any resemblance marks will result in the data being declined or transferred to a call centre for physical authentication. This development involves no extra hardware for the customers as all examinations are performed in the setting. However, this approach comes along with certain challenges, as there will be an escape or loophole in the technique when a fresh fraudulent incident arises that has yet to be identified. Moreover, occasionally legitimate transactions may be transferred to call centres, causing inconvenience to the users or customers.

Seventh, two-layered passwords constitute a universal technique of fraud prevention for verifying customers before letting them gain access to electronic banking systems. For verification to be successfully completed, customers are usually required to have separate internet banking passwords and usernames. Nevertheless, the regular use of a password for different prevention services leads to an increase in the vulnerability of electronic banking customers. Therefore, further methods of security are mainly for identity authentication (Moskovitch et al., 2009). However, Vandommele (2010) concluded that the conventional approach of authentication with password and username is inadequate and unsatisfactory.

Eighth, Biometric Approaches, is considered a progressive means of prevention and detection of fraud, due to the various distinctive characteristics of electronic banking users involved in recognition, verification and discovery. Vandommele (2010) discusses the various features of biometric technique: distinctiveness, universality, intransience,

intransigence, performance, circumvention, satisfactoriness and adequacy. Sarma and Singh (2010) also emphasized the resemblance characteristics of biometric technology that should be given great concern in its analysis and evaluation.

Ninth, Keystroke Dynamics is a method of analysing the user's approach to entering or typing personal information, passwords or accounting data in an e-banking channel by observing the keyboard input data, endeavouring to recognize this data as the usual beat system in the process of typing (Monrose, 2000). The keystroke approach is an innovative technique which was employed by the United States armed forces to differentiate friends from adversaries through Morse code and communication during the Second World War (Bartholomew, 2008).

Over the years, there have been a number of studies on the relevance and reliability of keystroke dynamics through changing input process and algorithm procedures. Patil and Renke (2016) conducted experiments on keystroke dynamic technique via passwords ranging between six and eight characters. Revett et al. (2005) investigated keystrokes using a passphrase of a regular number of 14 digits entered by every e-banking user. The authors calculated a resemblance measurement to form a decision chart and used this to evaluate the rules based on irregular sets. The surveys aimed to discover illegitimate and legitimate logins derived from the key-typing style of the e-banking users. These researchers' findings show (data tests showed 95% accuracy achieved) that the first and last characters, including the typing speed, are the major indicators for determining legitimate and illegitimate logins (Revett, Magalhaes & Santos, 2005).

In addition, research conducted on conciliation between the standard password and lengthy text input using passphrases techniques showed a 0.5% false acceptance rate and a 3.1% false rejection rate (Boechat et al., 2006). The algorithm in this investigation merely involved keystroke latency. However, Gunathilake et al. (2013) state that compared with other present techniques, keystroke dynamics are a highly efficient and prolific approach to validating internet schemes. The keystroke dynamic system is gainful for software, since it improves electronic system access protection; consequently, this

makes it also appropriate for reinforcement of the internal security of banks and particularly of electronic banking systems (Revett et al., 2005).

Correspondingly, some scholars have argued that among the various biometric systems, the keystroke dynamic network is the best and most appropriate method due to its cost-effective implementation and performance: it requires only software, and a keyboard and gives reasonable and adequate results over and above the higher rate of transparency it offers (Choras and Mroczkowski 2007). Revett (2009) opined that some banks have implemented keystroke dynamics as a main authentication tool while others have used keystroke dynamics software as a supplementary authentication method. Anthenware technology is a type of online security system protection software which works by understanding and learning the distinction between keystroke behaviours (Bergadano, Gunetti & Picardi, 2002). For instance, Ecuador Bank installed Authenware software to measure keystroke patterns and internet behaviour.

Tenth, bio-password is a type of security keystroke biometric software that operates through a neural algorithm for examination of data and the provision of Crossover Error Rate (COER) to the users. If it provides 3% COER, this means the software has the capacity to register users instantaneously, steadily and noiselessly. Additionally, Shanmugapriya and Padmavathy (2009) investigated the intrusion of the waiting time between pressing an input key and obtaining a result differentiating legitimate e-banking users in order to differentiate the legitimate e-banking users from illegitimate users through the use of a multilayer neural network approach. The neural network approach is a forecast model using historical events to envisage the result of a future event. The outcome proved that adopting neural network for differentiation resulted in a better outcome than any other statistical techniques.

Eleventh, Bhattacharyya et al. (2009) concluded that biometric authentication enhances the components of identification, non-repudiation and authentication in security information. Consequently, this technology has a fundamental role to play in e-banking fraud reduction. Biometric systems provide a way forward by considering individuals' distinctive features as a means of identification. Even though recent development and

improvement of biometric technologies, which include fingerprints, keystroke dynamics and iris recognition, appear promising, Murdoch and Anderson (2010) pointed out that authentication techniques for e-banking fraud prevention must be economically viable and technologically reliable. Many researchers, though, have proved the suitability and accuracy of biometric authentication for prevention of electronic banking fraud. Also, some organizations have implemented behavioural biometrics to enhance their security.

Twelfth, bank verification number (BVN) is a mechanism used to reduce the potential harm of fraud, every business organization, particularly the banking industry, must invest not only in advanced technology but also in policies and people for detecting and preventing attacks as promptly as possible. This has led the Nigerian Central Bank to introduce another policing method: The Bank Verification Number (BVN). Globally, biometric technology has been adopted to analyse human characteristics as an improved form of verification, authentication and certification for real-time security methods (Blass & Oved, 2003). In the face of cumulative occurrences of compromising, of orthodox security systems (PIN and password), the need for sophisticated security for access to personal and sensitive information in the banking industry has become inevitable.

Therefore, on 14 February 2014, the Central Bank of Nigeria, through the Bankers' Committee and in cooperation with all Nigerian Deposit Money Banks (DMB) and the Nigeria Inter-Bank Settlement System (NIBSS)), introduced a centralized biometric identification system for the banking sector, called the Bank Verification Number (BVN) (CBN, 2014). However, the aim of this project (BVN) is to protect bank customers from identity theft and other financial frauds emanating in the Nigerian banking industry (Orji, 2014). The current research will analyse the present mode of operation in the Nigerian banking industry, assessing the impact of the BVN since the date of introduction into the Nigerian electronic banking system.

Finally, ASSOCHAM (2015) in the investigation carried out on "Current fraud trends in the financial sector" found that the adoption of the following methods would enhance the rate of electronic bank fraud detection in the financial institutions. The methods of fraud risk management were adopted which are, whistle-blowing and tip-offs, suspicions

transaction reporting, internal audit, data analytics, by accident, by law enforcement, corporate security (physical and IT), investigative media and rotation of personnel. The author further explained that, fraud detective oversight must be in place such as, surveillance and monitoring systems (escalation and investigation, data management, program and controls testing), analysing identified red flags, regulatory and internal reporting, internal audit, independent review and investigations. While, Deloitte, (2015) opined that to accomplish effective detection of electronic fraud, there must be included of tool for electronic detection, forensic imaging, data anomaly discovery and information management tool which also supports banks and legal counsel for analyses and control complex information on the fraud cases.

2.8 Summary

This chapter has elucidated the most pertinent and suitable secondary information recognized by the researcher in the literature on the aspects of e-banking fraud prevention and detection which also included contextualising of the Nigerian banking sector which comprises its history, evolution and structure of the Nigerian banking system and historical background of e-banking services in Nigeria such as internet banking, mobile banking, telephone banking, ATM and other channels of banking and e-payment.

However, under the current guideline, licensed banks were approved to perform banking activities of their licensed category which grouped into three categories in relation to their activities, namely: Commercial Banking (Deposit Money Banks) License, Merchant Banking License and Specialized/Development Banking License. The chapter has also elucidated the impacts of e-banking fraud which are monetary and non-monetary impacts. While, personal data, educational information, health information, credential information, payment card data, financial information, others and unknown through hacking or malware, insider leaks, payment cards, fraud loss or theft and unintended disclosures are major information types targeted by e-fraudsters to defraud an individual or an organization.

In addition, the factors contribute to the increase of e-banking fraud were classified into technological factors and non-technological factors. And the prevention and detection mechanism were categorized into internal control, education, awareness, training, verification, rules and regulations, technological techniques, transaction monitoring strategy, two-layer password, application of biometric approach and keystroke,

CHAPTER THREE: THEORETICAL FRAMEWORK

3.0 Introduction

This section deliberates on the related studies to the phenomenon with the associated theories adopted so as to show light to the appropriate theories employed in this study. While, concluded with the discussion of routine activity theory (RAT) and fraud management lifecycle theory (FMLT) as the theoretical framework underpinning of this study.

3.1 Related Studies of E-banking Fraud Prevention and Detection

There are a small number of studies on fraud prevention and detection in electronic banking (Phua, Smith & Gayler, 2012; Dzomira, 2015). Most of them are fraud prevention, such as (Robert et al, 2009; Roberds 1998; Vandommele 2010; Bhattacharyya 2009; Murdoch & Anderson, 2010; Tan, 2003) which adopted efficient and effective security control to prevent counterfeit transactions perpetrated by fraudsters and to enhance integrity and honesty transactions. Alimolaei, 2015; Peotta et al. (2011); Kovach and Ruggiero, 2011; Bignell, 2006; Dandash, et al. (2008); Edge et al. (2007); Hertzum, Jrgensen, and Nrgaard (2004,); Leung, Yan and Fong, (2005); Aggelis (2006); Wei et al. (2013) and Edge et al. (2007) investigated on detection of internet banking fraud based on critical success factors and online banking security measure.

Furthermore, related studies on eletronic banking fraud prevention and detection, a number of research studies on only credit card fraud prevention and detection have been conducted (Alfuraih, Sui & McLeod 2002; Dheepa & Dhanapal, 2009; Mahdi, Rezaul & Rahman, 2010). A lot of the studies on the detection and prevention of credit card fraud have been done by using Neural Networks, Rule-Based Association System, Neuro-Adaptive Approach, HMM, BLAST-SSAHA Hybridization and other statistical

modelling (Kou, et al. 2004; Leung, Yan & Fong, 2004; Srivastava, et al. 2008, Neill & Moore, 2004). However, almost methods and theoretical frameworks of prevention and detection of credit card frauds used to identify spending forms which based on the only historical transactions are not suitable for the active banking industry as a result of various e-banking customers' transactions and the incomplete previous data obtainable from individual customers.

Notwithstanding, Chiezy and Onu (2013) appraised the effects of fraudulent activities on the growth and development of banks through data from 24 Nigerian commercial banks, between 2001 and 2011 (secondary source of data). The association between fraud incidents and other variables were appraised using multiple regression analysis and Pearson product moment correlation.

Moreover, some scholars based their studies on computer intrusion detection and prevention. For instance, these studies mainly examined the prevention and detection of anomaly and misuse of computer systems within the organisation by monitoring program behaviour, multiple classifier model and Neutral networks model (Beghdad, 2008; Ghosh et al, 2007; Eskin & Stolfo, 2007; Teoh det al. 2004; Giacinto, Roli & Didaci,2003). Therefore, since forensic financial investigators declared that detection and prevention of computer fraud is all about the users of computer systems, prevention and detection techniques of intrusion which are the attributes of electronic banking activities. Thus, the theoretical framework used could be applied to the e-banking fraud prevention and detection.

In addition, Mhamane and Lobo (2012) study investigated prevention and detection of online banking fraud with the adoption Hidden Markov Model (HMM) algorithm and Fraud Management Lifecycle Theory while, Wada and Odulaja (2012), Bossler and Holt (2009), Reyns, (2013), Wilhelm, (2004) and Leukfeldt, (2014) conducted qualitative studies on cybercrimes and internet banking fraud with the use of routine activity theory (RAT) and fraud management lifecycle theory (FMLT). The finding holds that the combination of the absence of a capable guardian with a suitable target and a motivated offender in a convergence of space and time has an influence on the victimization of

malware and phishing. Precisely, Wilhelm (2004), Jamieson, Stephens and Winchester, (2007) Newton; Nenga and Osiemo, (2013) investigated for fraud management and control with the use of fraud management lifecycle and their findings exposed that the proper interrelationship of distinct groups and components of these stages would result to successfully control and perfect management of fraud in the organizations. Hence, the theoretical framework of fraud management lifecycle theory was considered also useful and appropriate for this study.

Likewise, Jansen and Leukfeldt (2016) researched on "phishing and malware Attacks on online banking customers in the Netherlands", the qualitative analysis of the factors of victimization with data collected from 30 victims of malware and phishing in their bank accounts through semi-structured interview and using routing activity theory as a theoretical framework. The finding showed that victimizations of malware and phishing attacks were marginally influenced by suitable targets. In the same vein, Hutchings and Hayes (2009) investigated quantitative research on "routine activity theory and phishing victimisation". The study investigated 104 victims of deceptive email through the interview. The findings revealed that probable victims who perform routine activities through online banking and other computer activities are more vulnerable to be defrauded by motivated offenders.

In a nutshell, the theory of routine activities has been extensively used in the extant literatures, among other things, robbery (Tseloni, et al. 2004), sexual crimes (Tewksbury and Mustaine, 2001), cybercrime and online frauds (Newman & Clarke, 2003; Eck & Clarke, 2003; Wilsem, 2013; Holt & Bossler, 2008; Bossler et al., 2012; Pratt, Haltfreter & Reising, 2010, Williams et al, 2013; Reyns & Henson 2013). Likewise, Yar, (2005); Delvema, (2015) Choo, (2011); Willson and Fulmar (2014) and Bossler and Holt, 2003 discussed the cybercrime with application of mixed method and routine activities theory. Therefore, the theoretical framework of routine activity theory was also considered suitable and appropriate for this study.

Furthermore, the routine activity approach has been used by several studies of cybercrime (Ngo and Paternoster, 2011; Duffield & Grabosky, 2001; Hutchings & Hayes, 2009;

Reyns, Henson & Fisher, 2011; Van Wilsem, 2011). Therefore, the theory applies to this phenomenon. On the other hand, Pratt, Holtfreter and Reisig (2010) view through the suggestion of routine activity theory that those involved in e-banking is more likely to be victims of fraud. Karmen, (2010) opined that the victim of e-banking fraud is naturally involved in a lawful transaction and legitimate online business at the time of attack and oppression. Because of this, merely engaging in transacting business or transferring money (e-payment or e-commerce) from e-banking websites provide a high-fraud motive, compared to individuals or entities that do not transact business or pay money via e-banking.

However, out of the various channels of electronic banking, only online banking through phishing and malware and card payment fraud prevention has ever received concerns of the researchers, therefore, there is a need for examination of e-banking fraud prevention and detection with the use of routine activity theory (ROT) and fraud management lifecycle theory (FMLT). Hence, this study.

3.2 Theoretical Underpinning the Study

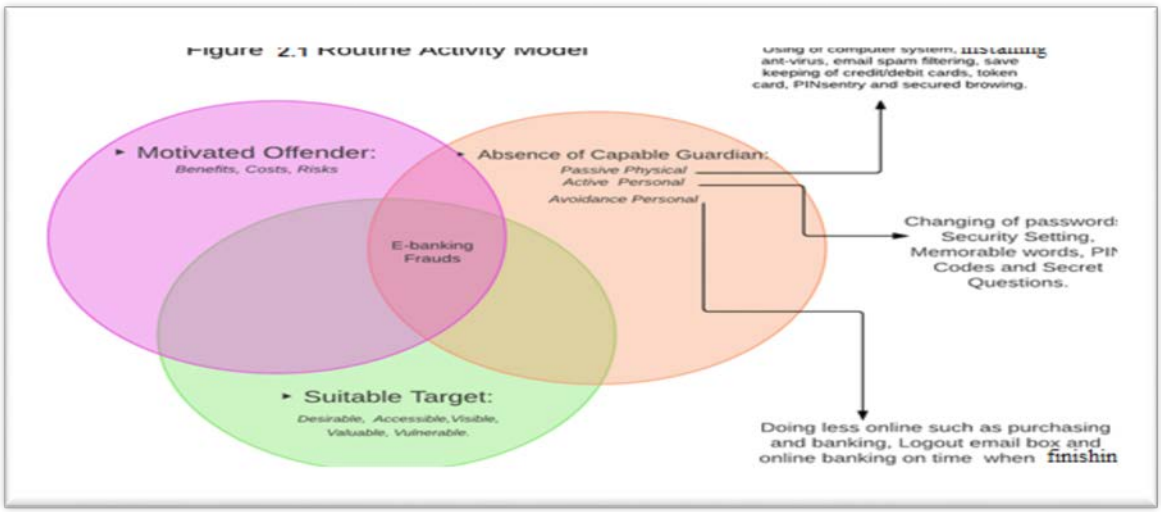
Over the past three decades, many theories have been developed to elucidate the nature of fraud. The two principal theories of criminology and management were adopted as theoretical frameworks that underpinning this study, which are the routine activity theory (RAT) and fraud management lifecycle theory (FMLT).

3.2.1 Routine Activity Theory (RAT)

A routine activity theory is a significant theory of environmental criminology and a place-based clarification of fraud theory, where the behavioural forms and the interrelationship of people in the place and in time influence where and when fraud occurs. The theory advocates that when suitable targets and motivated offenders meet without capable guardians, fraud will probably materialize (Miller, 2013). Equally, the non-appearance of any of these listed three circumstances might be sufficient to prevent a fraud from happening. Positioned within the comprehensive context of environmental criminology, routine activity theory proposes that reducing opportunities for fraudulent activities plays a significant role in minimizing the pervasiveness of fraud (Williams, 2016).

However, routine activity theory is, in a nutshell, an effort to identify fraudulent activities and their methods through clarification of vicissitudes in movements in the fraud rate (Cohen & Felson, 1979). It therefore offers a setting of orientation for material and modified fraud analysis and simplifies the application and implementation of actual practices and policies aimed at changing the essential elements that make the presence of fraud probable, thus averting it (Tilley, 2009) (see Figure 2.1).

Figure 3.1: Routine Activity Model



Source: Hutchings and Hayes, 2009.

The routine activity approach was introduced in the United States by Cohen and Felson (1979). This approach has proved its helpfulness in accounting and banking for a variation of fraudulent activities (Bradford, 2013). The routine activity theory was developed to examine the vicissitudes in the crime rate after World War II (Kennedy & Forde, 1990; Cohen & Felson, 1979). From the societal perspective, routine activity theory specifies that variations in combined routine activities can generate opportunities for fraud.

Furthermore, from the individual perspective, empirical researchers have emphasized the position of the individual or entity's routine activities in generating fraud opportunities (Fisher, Daigle & Cullen 2010). However, the routine activity theory proves that there is an opportunity for the occurrence of fraudulent activities in a place and time when the motivated offenders come together and there is availability of suitable targets with absence of capable guardianship. The proposal of a routine activity theory (proximity and acquaintance to target attractiveness, motivated offender, with absence of capable guardianship) has become the main elucidation of what brings individuals to fraud or being defrauded.

Moreover, the continued acceptance of the theory in clarifying direct-contact fraud incidence has prompted researchers to adopt the theory to describe opportunities for fraud taking place at a distance (Holtfreter, et al., 2010; Marcum, Higgins & Ricketts, 2010). The theories have mainly concentrated on fraudsters that meet their targets in a place (Tillyer & Eck, 2009). However, some frauds do not require direct and physical contact at a place. This has encouraged philosophers to determine whether the routine activities approach is restricted to place-based fraud (Tillyer & Eck, 2009).

In addition, the struggle of the first researchers to adapt the routine activity approach to frauds in which fraudsters and their victims do not meet in the same space and time have generated assorted, but inspiring results (Marcum, Higgins & Ricketts 2010; Holt & Bossler, 2009). These studies have concentrated on e-banking fraud, such as computer virus contagion and phishing harassment, and suggest that more studies are required for categorizing cyber routine activities that possibly place cyber operators at higher risks of diverse cyber fraud and adapting the theories to describe distance-based fraud. The

current research work discourses both phenomena through appraising e-banking fraud, prevention and detection from a routine activities perspective.

Correspondingly, in the context of e-banking fraud, routine activity theory (RAT) is an environmental theory, a time-and-place-based elucidation of crime, where connection of individuals and behavioural patterns of a place and time influence where and when frauds occur (Williams, 2016). The routine activity theory suggests that there is likelihood of fraud when there is the absence of a capable guardian and the availability of attractive targets and motivated offenders (Marcum, Higgins & Ricketts, 2010). Conversely, the absence of one of these elements might be able to stop e-fraud from occurring. Therefore, this theory is adopted by this study.

In this case, routine activity measures a diversity of hypothetical fraud environments, such as places and time spent on the internet. The following twelve routine activities are related to online identity fraud, which is classified into activities and locations of internet access that measure a variety of cyber activities and location access. The first group is cyber activities such as purchasing, banking, auction, selling, email and social networking. The second group is location of internet access, which includes bank, home, public, university, mobile, café and work; some locations are more dangerous than others, such as computers in public places and cafes that have many users, which can increase virus infection (Wilcox, Madensen & Tillyer, 2007).

However, if these approaches of internet activities remain unguarded, this will probably uncover attractive internet targets to motivate electronic fraudsters. The routine activity theory describes fraudulent activities through three important bases that meet in time and space in the sequence of daily events: (a) Capable guardian; (b) Suitable target; (c) Motivated offender.

3.2.1.1 Capable Guardian

The first element explained in this theory, is the absence of a capable guardian; that is, of someone or something that can intercede to prevent a fraud from happening (Cohen & Felson, 1979). The presence of a capable guardian will not permit the possible fraud to be committed, while the absence of a capable guardian will give room for the fraud to be committed. A capable guardian includes anyone within an environment or working as a guard of property or persons, such as security guards and police. They are honestly capable guardians and are usually absent when frauds are happening (Felson & Rachel, 2010). The study of the classic Kansas City Preventive Patrol Experiment, as reported by Kelling, et al (1974), established the efficacy of random patrols and concluded that an increase in the usual patrol rate in a certain environment had no significant impact on fraudulent activities in that environment.

Moreover, the house occupants, a brother, passer-by, or a friend – in short, anybody who is protecting his/her property or others' property and who may be important in preventing fraud – must be recognized as a capable guardian. However, a literature review of the capable guardian of routine activity theory has described guardianship as the symbolic or physical presence of a person or group of persons that acts either unintentionally or intentionally to prevent a potential fraudulent activity (Hollis-Peel, et al., 2011). For instance, closed-circuit television (CCTV), which is placed by people, but is a presence at the place of fraud that is not physically seen (Hollis-Peel et al., 2011). Felson (1995), in an effort to relate routine activity theory to Hirschi's social control theory (1969), polishes the image of the guardian by differentiating the place manager from the intimate handler. The place manager guardian is recognized as those individuals or persons who have guided and controlling responsibilities at a certain place; for instance, bus drivers, doormen, and the like.

The intimate handler may be a parent or family member who attempts, through condemnation and disagreement with the motivated offender's behaviour, to deter the actions that disrupt the rules. Thus, in extending at the notion of the capable guardian, Felson (1995) considered the four factors of Hirschi's theory which commitment,

attachment, belief, and involvement. The author abridges these factors into one: “handler”. Furthermore, analysing the idea that somebody could deter an offender through his/her presence in a place, or that a person could discourage a probable offender due to his relationship with him (Cohen & Felson, 1979), shows that control is an essential element in the fraud rate, and also that success of a place manager is based on the degree of relationship and responsibility he/she has with the possible offender.

Consequently, in the context of e-banking fraud, capable guardianship can be reflexive physical guardianship: operating only one electronic system, using antivirus and email spam filtering, safekeeping of credit/debit cards, token card, PINsentry and secured browsing. It can be active personal guardianship through the changing of passwords, security settings, memorable words, PIN codes and secret questions (Wilcox et al., 2007). Moreover, it can also be avoided personal guardianship: reducing time spent on the internet such as during online purchasing and online banking and logging out of email and electronic banking on time when finishing. If these online activities are well guarded, motivated electronic fraudsters may be deterred from suitable online targets to perpetrate electronic banking frauds.

Capable guardians include law enforcement, the owner of the property (the account holder), banks and other financial institutions, Computer Emergency Response Teams (CERTs) or any other agency or individual that is capable of discouraging the offenders (Yar, 2005). It may also be social-informal guardians such as systems security staff; in-house network administrators; and technological or physical guardians such as intrusion detection systems, virus scanning software, and firewalls (Denning, 2000).

As e-banking is often faced with attacks related more to characteristics of human nature than technical activities, a proficient guardian can be fashioned by feeding the customers with awareness and information rather than safety software. In addition, the Australian Crime and Security investigation posited that awareness may be missing. It was concluded in 2006 that even though 98% of responding companies considered antivirus and firewall software, only 15% of respondents agreed that they had got satisfactory training and skill through security and protection awareness (AusCERT, 2006).

In the same vein, the highest influence on e-banking fraud attacks was attributed to lack of qualitative staff education and adequate training in protection and security procedures and practices (AusCERT, 2006). Growing the public and collective awareness of possible fraud victimisation improves their capacity to become capable guardians. Grabosky and Smith (2001) stated the significant principle for preventing electronic fraud is the demand for the necessity of awareness of the potential victims to the menaces of fraud.

Smith and Akman (2008) appraised the 2007 campaign conducted by the Australasian Consumer Fraud Taskforce (ACFT), which was organized by 19 government departments and agencies for customer protection against fraud and related incidences and found that it was exceedingly effective in floating customer awareness. The campaign involved the circulation of flyers and posters, radio advertisements, media releases and television appearances, and included articles in magazines and newspapers (Smith & Akman, 2008). Therefore, the researchers also suggested that website cautions on internet browsing and banking websites, email filters, hints for identification of authentic and legitimate websites, and provision of procedures for suspected online fraud or hoax email reporting on banking websites will serve as capable guardians.

However, it seems as if the banking sector is not happy to be responsible for the role of capable guardian. Correspondingly, the Parliamentary Joint Committee on the Australian Crime Commission's (2004) investigation of cybercrime observed that a suggestion by the Association of Australian Bankers emphasized the customers' responsibility for personal-protection or self-safety from fraud rather than the banking industry's responsibility for protection and security of their customers. Therefore, while financial institutions will habitually recompense sufferers for their monetary losses, they are unwilling to take the issue any further. Lynch (2005) contended that there is no monetary incentive for the banking industry to prevent electronic fraud.

Nevertheless, recently there have been improvements in banking industries through using two-factor and three-factor identifications, whereby customers are required to use multiple techniques, such as a digital token and password (Smith, 2007). Reyns (2013), Wilsem (2013) and ENISA (2012) have tested the application of the routine activity

approach and the policy hypothesis of the adoption of passive physical guardianship and active personal guardianship in online crime and cyber victimization. Their findings show that the application of the routine activity approach reduces cybercrime and online identity theft.

3.2.1.2 Motivated Offender

This describes someone whose motive is to perpetrate fraud and who is capable of doing so (Cohen & Felson, 1979). It is possibly a young man, deprived of steady employment, a school dropout, as well as intelligent, canny and clever (Gottfredson & Hirschi, 1990). Even though in the original formulation of this theory by Cohen and Felson (1979) the term “motivated offender” was used, in later studies such as Felson & Rachel, 2010. The authors have avoided using the term “motivated” to describe the offender: what they considered relevant was not the motivation or the temperament to perpetrate a fraud, but rather the physical influences which made it probable for a potential fraudster or someone to be involved in perpetrating fraud.

Thus, what this tactic underwrote was an enunciation required to distract attention from the perpetrators in order to recognize and understand the fraud (Felson, 1995), Nevertheless, though it is essential to take note of other characteristics of fraud in order to prevent and understand it (Felson & Clarke, 1998), this does not mean forgetting the standpoint of the fraudster (Felson, 2008); the very explanation of the suitable target is through the acknowledge and understanding of the importance and capacities of the fraudster in relation to essential characteristics of the possible targets of fraud.

The sources of this perception can be discovered in the study of Cornish and Clarke (1986), which intersects with the approach of Felson (1995) in beginning from a point of rational decision and in laying emphasis on fraud prevention and elucidation of the environment in which the fraudster performs. The rational choice proposition is when fraudsters make decisions after they have assessed the availability of opportunities of perpetrating fraud successfully, the anticipated benefit attached to it and the danger of being caught. The motivated offender may be temperamentally inclined to perpetrate

fraud; that is, the person evaluates the diverse options available to accomplish targeted objectives, whether lawful or unlawful, and eventually chooses to start committing frauds. The motivated offender can be influenced by circumstances or conditional factors.

Nevertheless, the Cohen and Felson approach has been dependable and constant with the impression of a rational offender who takes the benefit of opportunities. At this point, the issue of opportunity has a significant role from the perspective of routine activities.

In fact, deviations in society's routine activities, the ineffectiveness and unreadiness of guardians, or the increase in obtainability of suitable targets may strengthen the probability of fraud if these elements meet in space and time and consequently create opportunities. In addition, another most significant and commanding concept in routine activity theory is indeed that opportunity is wrong or not evenly distributed in society, and therefore there are a restricted number of obtainable targets that the fraudsters may find suitable (Tillyer & Eck, 2009).

3.2.1.3 Suitable Target

This is the property, a person or any object that may be attractive to an offender. The likelihood that a target is more suitable or less suitable is a function of twelve attributes, designated from the perspective of the offender by the acronyms "CRAVED", which defines levels of obtainability, and "VIVA" which describes levels of risk and challenge (Felson, 2008). The acronym "CRAVED" represents Concealable, Removable, Available, Valuable, Enjoyable and Disposable (Clarke 1999) while, "VIVA" means Value, Inertia, Visibility and Accessibility (Sutton, 2009). Sutton (2009) compared the two acronyms and established that they deal with distinguishable attributes. Likewise, the author argues that the elements of VIVA describe the characteristics that draw attention, while the CRAVED elements relate to characteristics that make the attractive object available for fraudsters (Anderson, 2006). This current study is about the victim's characteristics that motivate fraudsters to perpetrate frauds; hence it adopts the VIVA acronym.

The first letter of the acronym, “Value”, means that the fraudsters are targeting an individual with a huge amount of money in their bank account. This has been proved by Harrell and Lynn (2013) study of cybercrime, which describes the correlation between the identity theft attack and the individual with a higher income. The “Inertia” simply means the weight, volume and size of the online item, or data that influence the technical specification, portability and accessibility of the target (Yar, 2005). Therefore, a small amount of money is more easily stolen on electronic channels than a huge amount of money. “Visibility” is operationalized as electronic banking activities. Studies to cybercrime show that activities such as e-purchasing, e-fund transfer, e-payment, online auctioning, social media and wrong disposal of computer system and its devices make targets become visible and suitable for fraudsters (Duffield & Grabosky, 2001; Holt & Bossler, 2009; Pratt, Holtfreter, & Reisig, 2010; Hutchings & Hayes, 2009).

Additionally, “Accessibility” is the factor such as a virus, weak software, lack of antivirus, weak password and so on that provides a way for the fraudsters to attack the targeted customers (Duffield & Grabosky, 2001). Accessibility is referred to as the ability and capability of the fraudsters to reach the target, perpetrate the fraud and get away with it (Felson, 1979); for example, unauthorized access to cyberspace through vulnerable encryption devices and weak passwords. The routine activity approach has been used by several studies of cybercrime (Ngo and Paternoster, 2011; Duffield & Grabosky, 2001; Hutchings & Hayes, 2009; Reyns, Henson & Fisher, 2011; Van Wilsem, 2011). Therefore, the theory applies to this phenomenon. On the other hand, Pratt, Holtfreter and Reisig (2010) view through the suggestion of routine activity theory that those involved in e-banking is more likely to be victims of fraud.

Karmen, (2010) opined that the victim of e-banking fraud is naturally involved in a lawful transaction and legitimate online business at the time of attack and oppression. Because of this, merely engaging in transacting business or transferring money (e-payment or e-commerce) from e-banking websites provide a high-fraud motive, compared to individuals or entities that do not transact business or pay money via e-banking. Although it is not illegitimate, the activity of procuring items by the means of

e-payments is not the norm. Snyder (2000) posits that the guardianship of online business transactions comes via three procedures: self-regulation and in-house discipline of the online business transaction; organizations and consumer protections; and government regulations. Guardianship does occur in all three procedures from the standpoints of e-fraud prevention and detection; therefore, this theory has really impacted on this phenomenon.

Finally, routine activity theory is one of the main theories used in this study. This section applies routine activity theory to the perception of a target assortment of e-fraudsters in e-banking fraud. In an e-banking fraud, "Suitable Targets" is the banks' websites and customers' account information that are involved in the malicious software configuration page to be targeted in e-banking attacks. "Motivated Offender" is the e-fraudster: the planner and the executor of the attack. The "Absence of Capable Guardian" is heightened by cyberspace's distinctive inconspicuousness and could be described as the absence of security countermeasures in the banks and on the part of the customers. Consequently, e-banking fraud occurs at the places where these three criteria intersect each other.

In conclusion, the theory of routine activities has been extensively used in extant literatures; among others, robbery (Tseloni, et al., 2004); sexual crimes (Tewksbury and Mustaine, 2001); and cybercrime and online frauds (Pratt, Holtfreter, and Reisig, 2010; Reyns, 2013). Conradt, (2012) has discussed the extrinsic and intrinsic features of cyberspace and deliberated whether it offers a diverse atmosphere of fraud opportunity.

Furthermore, the major arguments used to criticise routine activity theory interrogate its efficiency and efficacy, and its political and moral legitimacy, including its propensity to emphasize the victim's blameworthiness. However, these criticisms, which stem mainly from a certain category of authors associated with traditional criminology, respond to criticisms that theories of fraud generally and routine activity theory in particular is the only theories of frauds and the protective models (Cohen & Felson, 1979; Clarke & Felson 1993; Felson, 2008).

Additionally, critics have argued that routine activity theory is based on the rational decision, which makes it applicable only to insignificant crimes with a slighter emotional

element, and never to forceful crimes and frauds (Akers, 1998). Additionally, in relation to opportunity, it has been identified that routine activity theory and other fraud theories do not clarify whether spaces can change their capacity to perpetrate fraud or just stand as an attraction for frauds that would have happened anyway.

In conclusion, routine activity theory has faced its most unembellished criticism in the aspect of moral rightfulness. Its critics have shown that the emphasis on routine activities has revealed an ample absence of interest in the offender, therefore dismembering the aetiology of the challenge. In this case, routine activity theory, though it commences from the principle of the presence of a motivated offender, has not demarcated its connotation and has consequently been unable to demonstrate the basic methodologies of detecting frauds and to answer these questions: “Who are motivated offenders?” “What attributes do motivated offenders have?” and “Why are some people more interested and (motivated) than others to perpetrate frauds?” (Akers, 1998).

3.2.2 The Fraud Management Lifecycle Theory

The fraud management lifecycle is the proactive use of prevention, deterrence, investigation, policy, analysis, detection, mitigation and prosecution of the fraudsters (Wilhelm, 2004). The fraud management lifecycle theory is a network lifecycle where each node or stage in the lifecycle is a combined entity that is formed of interrelated and interdependent actions, operations and functions (Albrecht et al., 2010). The provision of this theory with its components will be adopted in the examination of electronic banking fraud prevention and detection in Nigerian banks. The adoption of this theory results from its methodical approach for combating frauds. In the first place, this theory creates an environment that deters people from perpetrating both online and offline frauds; it embraces the strategies to avoid frauds from happening; and even, if there is occurrence of fraud, and it has provision for purposeful detection strategy, it provides for reprimand and punishment of the criminals.

Moreover, Iminza, Gikiri & Kiragu (2015), in their study “Operational Governance and Occupational Fraud in Commercial Banks in Kenya: A Positivist Approach” proved that

the interconnections of the nodes or stages in the fraud management network are the main components of the fraud management lifecycle theory. The theory is significant; it vividly illustrations the stages of fraud management in a chronological manner and demonstrates what institutional procedures and practices should be installed in place for all kinds of frauds to be perfectly and effectively controlled. Furthermore, the theory assumes legal, uniform cultural and technological uses in the prevention and detection of fraud. Therefore, an operation of the Fraud Management Lifecycle begins with an explanation of the lifecycle platforms.

Devoid of this cognizance or consideration, fraud-managing professionals are not likely to relate efficiently with one another both within and without of the organization (Wilhelm, 2004; Jamieson, Stephens & Winchester, 2007; Newton & Osiemo, 2013). The theory posits that the proper interrelationship of diverse groups and components of these stages will result in successful control and perfect management of fraud in the organizations. Therefore, Wilhelm (2004) related the fraud management lifecycle with the need for the management to be responsible for reducing fraud chances and proactive in eliminating fraud opportunities; measuring and identifying fraud; and implementing and monitoring internal control, proper preventive and detective, and other deterrent measures.

Wilhelm (2004) describes the fraud management lifecycle as the accurate interconnectivity of stages of activities such as prosecution, investigation, policy, analysis, mitigation, detection, prevention and deterrence (see Figure 2.2 below), both internal and external to the business environment, to enhance an environment and culture that elevates ethical behaviour and promotion. This study will identify the effects of interaction of eight significant lifecycle stages in examining electronic banking fraud detection and prevention.

Figure 3.2: The Fraud Management Lifecycle

The operation of the management of the Fraud Management Lifecycle begins with elucidations of its components. One can equitably describe the several lifecycle platforms as numerous disciplines in fraud management. The Fraud Management Lifecycle is consequently a component in lifestyle; that is, a combined entity of interconnected, co-dependent, and self-governing functions, activities, operations and actions. These operations may, but need not essentially, happen in a sequential manner.

3.2.2.1 Deterrence

Deterrence is accomplished through creating fear of difficulty and consequences of perpetration, to discourage or turn aside fraudsters from attempting fraudulent activity (Kimani, 2013). Deterrence is characterized by activities and actions targeted at preventing and stopping fraud before it is attempted by making the effort to perpetrate fraud dreadful, unattractive or life-attacking (Ibor, 2016). Deterrence, the leading

component, is considered by functions, actions, operations and activities envisioned to prevent fraud before it occurs; specifically, to discourage the attempt at committing fraud. Examples include policy implementation, implementation of laws and regulations, card activation, internet passwords, card pin codes, anti-fraud portals, biometric identification systems, electronic passport verification portals, bank verification numbers (BVN), single points of connection with all bank schemes, data management programs and legal and reputational fraud management (Deloitte, 2015). Therefore, this should include establishing authentication measures and appropriate authorization privileges, physical and logical access maintenance, authentication control processes, customer verification, satisfactory infrastructure security to control appropriate restrictions and boundaries on both external and internal users, data and activities integrity of transactions, information and records.

3.2.2.2 Prevention

This is the second component of the fraud management lifecycle; this comprises functions to avert fraud from happening (Wilhelm, 2004). Prevention includes activities and actions to stop fraud from occurring (Ibor, 2016). Prevention should be supreme in any e-banking fraud control system. E-banking fraud prevention is the actions and activities to reduce opportunities for e-banking fraud to happen, such as the bank verification number (BVN). It must be centred on a fraud assessment development that reflects the bank's vulnerability to fraudulent activities within an integrated e-banking approach (Vasiu, 2004). Prevention is the activities to reduce the incidence of electronic fraud, which include core process components, automated controls, deep learning technology, data analytics, employee and customer education, fraud assessment, hotlines mechanisms and real-time monitoring (Chakrabarty, 2013).

3.2.2.3 Detection

This is the activity or action that reveals or uncovers the presence or attempt at fraud, such as statistical monitoring programs that are used to locate and identify fraud subsequent, during and prior to the completion of the fraud perpetration (Wilhelm, 2004).

Deloitte (2015) states that detection is a function or an activity exposing or disclosing the existence of fraud and fraud perpetrators which involves special tools and techniques, such as security monitoring software, security monitoring teams (forensic accountants, police forces), inter-agency problem bank meetings, statistical monitoring programs, and national anti-fraud programmes that are used to pinpoint and discover fraud early in, during, and after the finishing point of the fraudulent activity. Chakrabarty (2013) further explained that fraud detection oversight must be in place, for example through surveillance and monitoring systems (escalation and investigation, data management, program and controls testing), analysing identified red flags, regulatory and internal reporting, internal audits, independent reviews, investigations, fraud management, whistleblowing and tip-offs, suspicious transaction reporting, internal audits, data analytics, by accident, by law enforcement, corporate security (physical and IT), investigative media, and rotation of personnel.

3.2.2.4 Mitigation

This component aims to discontinue fraudsters' activities or to hinder fraud perpetrators from completing or continuing to perpetrate fraud by deactivating banking cards (credit or debit cards), barring their account passcode or PIN, or blocking an account; it can be achieved through message authentication, one-time passwords (OTPs), personal identification numbers, biometric characteristics, payment authentication codes to be sent to customers, customer awareness, customer verification, and account origination (Thamizhchelvy & Geetha, 2012; European Central Bank, 2013). In the following stage, known as analysis, losses that happened regardless of deterrence, detection, and prevention components are known and measured to control the causes of the damage situation by using statistical methods (Wilhelm, 2004).

3.2.2.5 Analysis

Analysis is recognised as the activities to understand and identify losses that happened regardless of the detection, deterrent, mitigation and prevention of e-banking fraud. Analysis must be performed to examine the effects of the fraud management stages of

activities on banks and victim customers. The cost of fraud incidences must be assessed and properly estimated to ascertain exert prioritization of fraud cases. The analysis component collects data concerning performance from other components of the fraud management lifecycle and feedback the outcomes of the performance of each of the components. The analysis gives the performance reporting matrices that permit fraud management to provide calculated, relevant, informed decisions. The procedures of analysis involve examination of causes and the volume of shortages or losses, the reporting and examination of investigation and performance analysis, reporting and evaluation of aggregate and individual detection (rule) performance, the examination and feedback on e-banking fraud prevention and detection, analysis of the impact of the aggregate or individual stages of the fraud management on the increase factors, prevention and detection mechanisms of e-banking fraud.

3.2.2.6 Policy

This is the stage of the fraud management lifecycle theory which deals with the creation, evaluation, communication, and deployment of policies to minimize the occurrence of frauds. Nance and Straub (1988) agreed that information security policies about organizational policies will prevent potential fraudulent acts from being committed. Hollinger and Clark's (1983) study demonstrates the significance of policy development and organizational control in the prevention of fraud and fraudulent activities in an organization. This theory suggests four key areas of policy improvement that are indispensable in preventing frauds: the full understanding of fraudsters' behaviour, the dissemination of useful information on organizational policy, broadcasting sanctions, and the implementation and enforcement of sanctions (Wilhelm, 2004).

This also implies that financial institutions need to employ the right, high-integrity, people as staff and have judicious expectations of them. Therefore, the theory postulates the effective and perfect control and management of fraud. Fraudulent behaviour and intentions need to be influenced through the adoption of effective organizational policies

and controls targeted at fraudulent awareness for deterrence and the development of controls to detect, prevent and deter fraudulent activities. The policy must strive for balance in deterrence value, sales volume, loss reduction, cost-effectiveness and operational scalability (Wright, 2007). Policy development encompasses continually reassembling the circumstances disassembled in the analysis stage, by gripping the benefit of the knowledge acquired by analysis and merging it with interactive, external and internal environmental factors with the purpose of crafting policies that address the whole intended situations (Wilhelm, 2004).

3.2.2.7 Investigation

This stage involves having sufficient information and enough evidence to end fraudulent incidents, recover stolen assets, and produce evidence that will support the prosecution and conviction of the fraud perpetrators (Wilhelm, 2004; Albrecht et al., 2009). Fraud investigations are concentrated upon three main aspects of activity: law enforcement harmonization, internal investigations, and external investigations. Law enforcement harmonization, as argued by Gottschalk (2010), is the maintenance and delivery of resources and information to the national, state, provincial and resident law enforcement authorities. Routine and rigorous investigation is required for an effective relationship with law enforcement to enhance effective deterrence of frauds. External investigations are carried out on fraudsters, organized groups, and customers. Meanwhile, internal investigations consist of investigating employees, managements, contractors, vendors, and consultants (Wilhelm, 2004). Electronic surveillance is one of the methods used in this stage of investigation.

3.2.2.8 Prosecution

Wilhelm (2004) argued that “Prosecution” focuses on the judicial and prosecutorial system of authority, along with law enforcement. The main objectives of prosecution in the arena of fraud are to discipline and castigate the fraudsters with the aims of preventing further theft; establishing, maintaining and enhancing the banking sector’s reputation; and deterring fraud incidence (Albrecht et al., 2009). The prosecution is the conclusion of

both positive and negative outcomes of the fraud management lifecycle stages. Outcomes are negative if the fraud was successfully committed and positive if the fraud was detected and a fraudster was identified, arrested, detained, and charged. This stage also comprises criminal restitution, asset recovery, and conviction with its attendant deterrent value. Wilhelm (2004) also recommends that the prevention and detection of frauds requires a complete fraud management lifecycle and effective connectivity of its components, which encompass deterrence, detection, prevention, analysis, policy, mitigation, investigation and prosecution. This means that effective management and control of fraud needs a balancing of the complementary and competing components of the fraud management lifecycle in financial institutions.

Failure to effectively balance the components of this fraud management lifecycle, and failure to adopt appropriate techniques that will ensure perfect integration of its components, may result in poor control and management of fraud in financial institutions. Therefore, the fraud management lifecycle can be said to be the fraud management, network, in which each of its components represents a node and the lifecycle represents a network, which is seen as a group of entities that is made up of interdependent and interrelated functions, operations, and actions (Wilhelm, 2014).

Moreover, for the fraud management lifecycle to be effective for controlling fraud, there must be an effective, systematic approach and standard coordination of the interconnection of its components. This indicates that, without detection of fraud, prosecution and punishment measures cannot be used to deter perpetration of fraud. An increased detection rate implies that deterrence and preventive techniques have failed. This signifies and confirms the importance of the relationship between these components. The theoretical framework of this study is based on the fraud management lifecycle approach; it will therefore examine the activities of deterrence, detection, prevention, mitigation, policy, analysis, prosecution, and investigation, including their combined interactions and their general impact on prevention and detection of electronic banking fraud in Nigeria.

However, some scholars have argued in their studies that e-banking frauds are not accidental occurrences (Gillett and Uddin, 2005, Bagnoli & Watts, 2010, Carpenter and Reimers, 2005). Numerous factors contribute to the possibility of their incidence, and the process of the incidence (Langenderfer & Shimp, 2001, ACFE, 2015, Bakre 2007, Zahra, 2005). Conversely, Wesley (2004) argues that the fraud management lifecycle theory is a lifestyle with a system made up of interdependent, interrelated and independent operations, actions and functions. As said earlier, fraud management lifecycle theory comprises eight stages: detection, deterrence, mitigation, prevention, policy, analysis, investigation and prosecution. Contrasting with the fraud triangle theory, Wesley (2004) opined that fraud management theory activities or stages do not essentially occur in a linear flow or sequence. The theory also makes provision for countermeasure of any type of fraud, either e-fraud or non-e-fraud.

Wilhelm (2004) consented with deterrence of frauds, prevention of frauds, detection of frauds, mitigation of frauds, analysis of frauds, fraud policy, investigation of frauds and prosecution of frauds. These platforms of the fraud management cycle must be carefully and successfully incorporated and balanced to get the advantages or the merits of developments in fraud detection and prevention technologies, to prevent the Nigerian economy from suffering shortages of valuable resources and to protect the Nigerian banking sector from fraudulent activities.

3.3 Summary

The relevant and appropriate secondary information acknowledged by the researcher in the literature on the aspects of e-banking fraud were discussed this chapter. The theories of fraud have produced an understanding of the methods, behaviour and characteristics of fraud and fraudsters. The related studies to the phenomenon with the associated theories adopted serve as guide fo the selection of appropriate theories employed as the theoretical framework underpinning this study which are routine activity theory (RAT) and fraud management lifecycle theory (FMLT).

However, a routine activity theory is a significant theory of environmental criminology and a place-based clarification of fraud theory, in which the behavioural forms and the interrelationships between people in place and in time influence where and when fraud occurs. It advocates that when suitable targets and motivated offenders meet without capable guardians, fraud will probably materialise.

Secondly, the fraud management lifecycle theory is the proactive use of prevention, deterrence, investigation, policy, analysis, detection, mitigation and prosecution of the fraudsters. It is a network lifecycle where each node or stage in the lifecycle is a combined entity that is formed of interrelated and interdependent actions, operations and functions. The adoption of this theory resulted from its methodical approach for combating fraud. In the first place, this theory creates an environment that deters people from perpetrating both online and offline frauds; it embraces strategies to prevent frauds from happening; and if there is occurrence of fraud, it has provision for purposeful detection strategy, reprimand and punishment of the criminals.

CHAPTER FOUR: RESEARCH METHODOLOGY

4.0 Introduction

This chapter elucidates the methodology and methods adopted for the research design by discussing the research philosophy, which involves epistemological position, ontological position, axiology positions and postmodernism. This chapter extensively describes the application of triangulation in this research design. It also explains population, sampling strategy, research instrument design and the data collection and testing procedures for this study. Data preparation and analysis procedure, factor analysis, structural equation modelling (SEM) validity and ethics in research will also obviously be discussed.

4.1 Research Philosophy

Research philosophy is known to be the foundation of any research; the core standpoints of the research philosophy control the researcher in making the right and sustainable decisions on the techniques and procedures of the data collection and in answering the research questions (Bridges & Smith, 2007). The justification of selecting certain methods and methodology is not only grounded on the research questions of the study, but also on the assumptions made about reality and theoretical perspectives. The theoretical approach enhances the choice of methodology and reproduces the philosophical substances that influence this choice. Theoretical assumptions influence understanding about human knowledge and its requirements. Theoretical perspectives, in contrast, involve knowledge by ontology and epistemology (Crotty, 1998).

Thus, the methods adopted in this research study are guided by the methodology, which is informed by the theoretical perspectives that are themselves influenced by the ontology or epistemology. Therefore, the philosophy of this research depends on the research onion, which is predominantly grouped into axiology, epistemology and ontology. In an endeavour to position this research work with a suitable philosophical framework, an attempt has been made to employ the research onion. In developing business and financial research, the main frameworks that are common and general for research methodology

are the research onion and the nested model (Saunders, Lewis & Thornhill, 2015; Omotayo & Kulatunga, 2015).

These frameworks have similar processes needed for effective research work, but the research onion was employed for this study because it has more explanatory research elements than the nested model. The research onion simplifies the research philosophy by breaking it into different platforms, from the research philosophies to the procedures and techniques (see Figure 4.1). This research methodology framework was used because of the research objectives and the choice of the researcher.

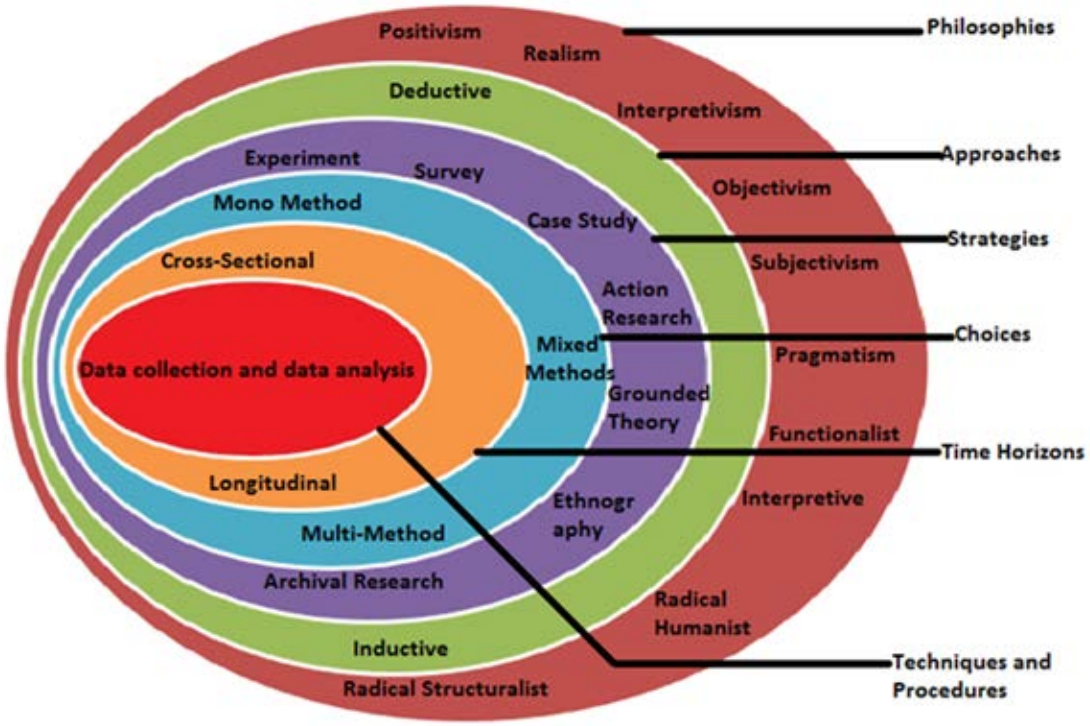


Figure 4.1: The Research Onion

4.2 Ontology, Epistemology and Axiology Positions

This section discusses the research philosophy of ontology, epistemology and axiology positions and their relationships and implications in the research methodology of this study.

4.2.1 Ontology

Ontology tries to discover if knowledge is the result or outcome of the mind; in this case it points to idealism and realism (Omotayo & Kulatunga, 2015). Idealism is a philosophical tactic that has the essential idea that belief is the merely factual reality, the single substance worth knowing. In idealism, the aim of this study is to examine electronic banking fraud prevention and detection to develop policies and other strategies that will prevent and detect fraud in the Nigerian financial institutions. While, realism is both a metaphysical and epistemological principles. If realism believes that in any case, some objects of held through observation are public, not private is known as epistemological principle. It is a metaphysical principle believes that object existence is mind-independent which means it is being neither experienced nor perceived by anyone. Realism can be viewed in this study as being inside and outside the social phenomenon of certain of the objectives.

Therefore, some literature was reviewed, and interviews and questionnaires were administered to get data about electronic banking fraud prevention and detection. The ontological world is the everyday live event (Lawson, 2004). It comprises people, their decisions and their experiences. In this study, it is the platform of electronic banking fraud prevention and detection in banks, which is the main duty of forensic accountants and auditors' everyday life. The research problem discourses a need in this platform; that is, examination of electronic banking fraud prevention and detection. To discover an answer to this research problem, the researcher is called to develop an epistemology.

4.2.2 Epistemology

Epistemology is the philosophy that discusses how to acknowledge, recognize, identify or develop knowledge (Hill, 1984; Holden & Lynch, 2004). Epistemology accepts other ways of approaching research (Khin & Heng 2012). Khin and Heng (2012) agree that

epistemology can be subjective as well be objective. The subjective idea of the epistemology is that the outer world is the territory of amplifications or illuminations from reflection, while the objective motive behind epistemology identifies the outer world, which is hypothetically impartial.

Furthermore, epistemology is a platform of scientific knowledge which contains data, findings, definitions, concepts and theories of phenomena with recognizable research problems; in this case, examination of electronic banking fraud prevention and detection in Nigerian banks. The two sides of epistemology are interpretivism and positivism.

The epistemological perceptions of positivism and interpretivism were both applied to the research objectives of this study: positivism is required for the evaluation and analysis, which will be used and be added to the existing literature, while interpretivism is involved as the stakeholders' experiences and opinions will also be needed. Saunders, Lewis and Thornhill (2009) posited that the researcher can include his or her own personal ideas or be determined not to be biased as to the value of the research or its concepts.

The philosophical orientation of the researcher stimulates his or her actions or values and involvement within the different platforms (Holden & Lynch, 2004). The following section will be dedicated to a review of various philosophical paradigms with the aim of placing the current research within a suitable or proper philosophical perspective. Specifically, there are three prevailing paradigms that make up the philosophical world, all of which are prominent or protuberant in all current-day social management research: positivism (the scientific or quantitative paradigm), phenomenology (interpretivism) and postmodernism (Onwuegbuzie, Leech & Collins, 2012).

However, in postmodern practice, theories take various narratives and literary forms (Khin & Heng, 2012). This is not excluded from surveys, historical analysis and essays, field research and case studies. Hence, in line with Bryman and Bell (2015), despite differences of methodology, this study adopts critical theory or postmodern theory and dialectical analysis, which obviously distinguish interpretivism or phenomenology and positivism from postmodern research.

4.2.2.1 The Positivism Approach

Positivist research uses quantitative methods, which include experiments, simulations and surveys (Holden & Lynch, 2004). Positivism is an objective platform (Krauss, 2005); therefore, it examines the facts, perceived in relation to the specific associations and correlations within the variables. Positivism is the position in which a scientific technique can be more significant and can measure, and it is used to forecast and discuss causal relationships among basic variables (Collis & Hussey, 2009).

Furthermore, positivism generally focuses on the quantitative and experimental methods that are used to verify and test hypotheses; these sometimes can be extended by an interested researcher by using qualitative methods to collect more data to measure outer limit of the intended measured variables (Saunders, Lewis & Thornhill, 2012). Positivism is the first scientific technique theory which believes that the observed and physical worlds can be quantitatively evaluated, the effects and causes can be identified and described with predictability and inevitability (Schutt, 2003). This philosophy originates in numerical research and predominantly in the analysis of statistical influences between phenomena as observed and measured.

1. Moreover, the positivist approach involves consistency and careful research design built on logical and reasonable assumptions and adoption of valid statistical comparison and measurement to achieve careful and thoughtful conclusions (Trochim & O'Donnelly, 2006). The positivist approach explains the world by generating common lawswhich can be can be measured and observed as facts and realities (Henn, Weinstein & Foard, 2009). Hence, the positivisms approach is extremely appropriate for statistical research study and for the discovery of effects and causes of associations or relationships.

   In addition, in the positivisms approach the observation of the phenomenon being investigated is made before the development of the theory based on this observation through a continuous process of observation and verification of comparable phenomena, positivism develops a theory that eventually turns out to be a law which can be comprehended and generalized to comparable phenomena. Paradoxically, the unceasing

verification and observation process that describes the positivist approach is also its drawback and downside as it restricts the advancement of knowledge and there could be restrictions created by observation.

Thus Henn, Weinstein and Foard (2009) position the resolution to these identified limitations "not in endeavouring to validate what we have previously known, but in endeavouring to falsify it." By this means, theories can be verified against fresh data and the typical application of a theory can be tested to see if the data disprove it. However, in the current research what can be tested may be restricted since, e-banking fraud is a compound problematic subject: it is indescribable by nature, so it may be difficult to correctly test features of e-banking fraud.

The positivist approach ignores or disdains any likelihood that the respondents or researcher may cause bias in the research work (Schutt, 2003). However, in the view of this researcher, such a postulation is exceedingly unlikely, particularly regarding the provocative issue of e-banking fraud. Therefore, a post-positivist approach was carefully selected for possibility of respondent and researcher been bias (Bracken, 2010). In this perception, it is recognized that there are external facts and objectives, that these can be measured and observed, and that these external facts and objectives lead into the approaches of scientific investigation (Grix, 2004).

However, there are also notifications that in any type of social investigation, the reality of objectives or facts does not remove the probability that human relations and explanations play a substantial role in creating subjective truth (Grix, 2004). Therefore, in this theoretical approach, there is no competition between recognizing the presence of objective facts and the potential for social creation of reality and knowledge.

Consequently, the realisms approach permits using of positivisms consistency in the research study but will also acknowledge the strengths of human bias and the influence of imperfect former research (Trochim & O'Donnelly, 2006). Moreover, this requires re-investigation of the investigation instruments in relation with outcomes and findings. This realism approach is extensively used accounting and management, in which virtuous

financial and statistical information have be merged with evidence and information concerning the enthusiasms of participants and researcher (Fleetwood, 1999).

However, distinct from the qualitative approach (best used with small samples, comparatively based on the description and unstructured), the quantitative approach is appropriate for a study that has a moderately large sample size, is extremely structured and is grounded in statistics. The belief behind qualitative research is that its richness in explaining the social world is valuable, while quantitative research is based on the belief that details interrupt the procedure of generalizing and oversimplifications (Denzin & Lincoln, 2003). In addition, in the positivist approach, rigour and objectivity replace experience and intuition as the resources for examining research problems (Colins & Hussey, 2009). Although the use of quantitative instruments such as questionnaires in the positivist method limits participants to what has been required of them, greatly restricting the opinions and views offered. One of the advantages of using this method (quantitative technique) is that, it evaluates the response of large population samples to a certain number of questions, simplifying assessments and permitting generalization and comprehensive of findings (Patton, 1990).

4.2.2.2 The Interpretivism Approach

The interpretive approach tries to enhance the collective understanding of reality; hence the personal experience and the ideas of the researcher and opinions or ideas of the stakeholders are included in the study. The objective of the researcher is not just to discuss the specific associations or the relationships between the variables being studied, but to determine what these associations or relationships mean in the situation of the overall Nigerian banking system. Nevertheless, positivist approaches do not permit the nature of interpretation needed to back up the requirements of research.

Hence, as this study adopts dual research approaches of positivism and interpretivism. The interpretivism approach is required to produce a better design. Interpretivism approach is useful and valuable in the social world, which assumes of the inherently subjective, which humans and research are derived from (Grix, 2004).

Interpretivism data produce a place to establish transparently grounds, deep descriptions and productive explanations of the processes in recognizable local or primary contexts of the phenomenon. It also gives an insight into unpredicted research outcome and develop associations for confirming theoretical contexts (Miles & Huberman, 1994). The interpretive approach investigation underlines an effort to acknowledge and recognize social phenomenon by generating meaning from experiences of the research participants or contributors.

Therefore, individual's knowledge and understanding are described from the personal perception or world perspective. Interpretivists search for understanding of how people attach meaning to their situations. The interpretivism (qualitative) approach describe social nature of reality and connexion amid the study and the researchers: "interpretivists find solutions to research questions which describe how social experience is constructed and provided meaningful interpretation (Denzin and Lincoln 2003). Interpretivism (qualitative) approach permits interviewees to state their views and opinions on e-banking fraud prevention and detection in the banking sector, permitting their interpretations and opinions to take precedence over those of the researcher.

Moreover, by considering the fraud experiences of the interview respondents, the researcher will be able to select out the important words in the responses and comments made by the interviewees. In the interpretative approach, participants can describe or interpret the world with their own ideas and words. As said "Language recognizes as an instrument with which we make meanings" (Henn, Weinstein & Foard, 2009).

Additionally, in an interpretive research approach, the contributor is active and represents inward competences which let individual sensitivities, perception, judgements and awareness to not just be passive instrument in the research. The respondents can contribute, change and influence the meanings of findings. Blumer (1969) advocates that, the distinctive characteristics of human behaviour are not based on people's behaviour to each other; instead they are based on people's interpretations of each other's behaviour.

Thus, interpretive approach includes researching on people and with people. Human behaviour understood but only by linking it to cognisant intents, purposes, motives and

eventually the standards of the agent that does it (Henn, Weinstein & Foard, 2009). Therefore, interpretivists contend that social realisms depend on what individuals think, say and do (Garrick, 1999).

According to interpretivism's supporters, there is no unqualified or absolute response from interpretivism participants (Candy,1991). Therefore, authors have also posited that due to the variety of social realities, and how and in what way they are experienced, constructed and known, social theories are ungeneralised globally as they are precise to known historic and cultural established norms (Grix, 2004).

Therefore, it is known that interpretivism regards the research procedure as a collaboration between the participants and the researcher, who become players or stakeholders. According to Onwuegbuzie, Leech and Collins (2012), "In qualitative analysis approach, the researchers are regarded as the tools." This is corroborated by Krauss (2005), who stated that researchers are substantial instruments of research; therefore, they must regard themselves as a vital tool of research in the interpretivist approach.

This qualifies the interpretivisms approach as suitable for certain research problems under investigation in this thesis. Interpretivism approach acknowledges the procedures or methods which individual participants make use of their words and intelligence. Moreover, it permits the researcher to perform in acquaintance with less ambiguous feedbacks or responses. Given the broad and complex nature of sensitivity of the subject of e-banking fraud, the interpretive research approach is appropriate and relevant for this study.

E-banking fraud in the Nigerian banking sector has also not been extensively studied academically, making it an under- or undeveloped research topic. Therefore, the interpretivist approach may be the best research approach to build up or explore an understanding of issues such as fraud, of which, in the researcher's view, little or nothing is known (Henn, Weinstein & Foard, 2009). In addition, this is also an area where it may be anticipated that present theory recommends the making up or use of narratives.

4.2.3 Axiology

Axiology deals with the value judgement of the researcher (Bryman, 2012). Therefore, the two sides of axiology may be considered: value-laden and value-neutral. These two sides of axiology relate to positivism and interpretivism in epistemology: positivism is interrelated to value-neutral, while interpretivism is interconnected to value-laden. Hence, in this study, a combination of the two was adopted due to the nature of the research objectives.

4.3 Postmodernism and Interpretivism versus Positivism

The supremacy of positivism in management and social research has been progressively challenged by its critics. Advocates of postmodernism and interpretivism supporters have made universal philosophical critiques of positivism and set out substitute theoretical and practical tactics and methodological approaches for social sciences and management research. They disagree with positivism because its meanings are rooted in the procedure of quantifying the measures of the phenomena (Collis & Hussey, 2009). David and Sutton (2004) state that the examination of ontological peculiarity is an essential method in the process of research because it assists the researchers in disclosing how the observation of the human environment impacts on the method deliberately adopted to uncover the social truths.

However, this study is built on epistemology and rooted in the ontological approach which believes that human behaviour is subject to the rules and orders that govern and control its external authenticity. That is the nature of existence. Also, there is a theoretical perception that human actions and behaviours are the function of natural stimuli or incentives (Bracken, 2010). Many researchers have argued that the kind of research methodology produced by positivist epistemology has limitations. For example, it cannot make an obvious distinction between human knowledge and non-human and non-animate

knowledge. The relationship of the positivist approach with the social sciences overlooks the impact of human agency.

Therefore, mixed methods are employed in this study to achieve convergence and adequate findings and to enhance the validity of the research findings (Trochim & O'Donnelly, 2006). This decision was taken because of the nature of this study: it includes the independence of the observer, asking questions about the significance of human actions and interested in such questions as how, who, where, why and when. These are simply known as phenomenological indices, as well as positivistic indices which involve theoretical abstraction, large sample size, collective understanding of physical and technological environments (Omoteso, 2006).

The broadest explanation of the phenomenon studied is produced by mixed methods, approaches through comprehensive elucidation of the studied phenomenon (which is simply known as a fraud) by producing several perceptions of it. This mixed methods approach will be adopted for full understanding and acknowledgement of e-banking frauds within banking, finance, auditing, the internet, technology and the human environment. Bryman, (2006), Collins et al. (2006) and Rocco et al. (2003) supported a mixed method approach as the best approach to social research for the following reasons: it enhances accuracy and it shows the full picture of research strengths and weaknesses, including provision of clear and complete analysis (Denscombe, 2008).

4.4 Triangulation

Triangulation, an idea presented by Webb et al. (1966) and then adopted for qualitative examination in Denzin (1978), applied the concept of observing a phenomenon from a diversity points of view. The notion was used in the arenas of navigation and physical research; it was found that it is not different within the understanding of the research methodology. For Campbell and Fiske (1959) and Bryman (2004), the triangulation positions the importance of the mixed method approach. The combination of interpretivist and positivist methods in research on a single phenomenon is popularly known as triangulation.

Amaratunga et al. (2002) posited that the triangulation method is also a mixed method, which mitigates the weaknesses of quantitative and qualitative methods by enabling them to strengthen each other. The authors proceeded to claim that this research approach can be inductive and deductive. This was corroborated by Saunders, Lewis and Thornhill (2015), who viewed triangulation as the use of more than one data collection method or independent sources of data within a study so as to ensure that data collected are telling you what you intended to say. The deductive approach is based on positivism, while the inductive approach stands on interpretivism from the epistemological perspective (Kadushin, Sasson & Saxe, 2008). The major function of triangulation in qualitative research is to enhance the validity and credibility of the research outcome. Cohen and Mansion (2000) describe triangulation as a map-out that studies the complexity and the richness of human behaviour through several perspectives. Bryman (2004) agrees that triangulation provides a balanced and clear picture of the situations.

The triangulation serves two major purposes in this study: it validates the findings and it expounds the level of understanding of the prevention and detection of electronic banking frauds by employing many perspectives in the data collection. Two types of triangulation methods, within-method triangulation and cross-method triangulation (Bryman & Bell, 2015) were considered for this research work. Within-method triangulation combines techniques for the same research strategy, while, cross-method triangulation is the combination of both quantitative and qualitative research strategies (Bryman & Bell, 2016). Likewise, mixed method research is the amalgamation of quantitative and qualitative research techniques.

Denzin (1978) suggested five kinds of triangulation that are more important to researchers: data triangulation, theoretical triangulation, methodological triangulation, investigator triangulation and environmental triangulation. Triangulation is suited for this research, since it employs both questionnaire and interview survey techniques to gather data, adopts appropriate quantitative and qualitative data analysis methods, employed criminology and management theories and applies different data collection techniques.

Therefore, triangulation is adopted because this research work includes numerous sources of data that are concerned with people, time, place and technology. For instance, bank staff and customers from various deposit money banks are interviewed and included in the questionnaire survey that was distributed and administered at distinct locations and various times. Gathering data from diverse sources and relating data from different respondents through the questionnaires and interviews enhances and proves the validity, reliability, conformability and the authenticity of the findings.

Theory triangulation was considered for this study as it employs many related theoretical approaches – the routine activity theory (RAT) and Fraud management lifecycle theory (FMLT) for the interpretation of the fraud detection and prevention phenomenon. Also, different can bring out the image and share the picture of the type of data collected and the manner of analysis and interpretation (Denscombe, 2008).

Methodological triangulation is also valuable to this study as it includes different methods of data gathering, analysis and interpretation. Attrichter et al. (2008) and Bryman and Bell (2007) opined that triangulation is useful for a survey where there is the expectation of a low response rate. This was the nature of this study, which comprised responses of core professionals such as bankers, accounting practitioners and information communication technology experts who are always busy; therefore it was decided by the researcher that a mixed method of both quantitative and qualitative was the most suitable as the possibility of getting a higher response rate would be greatly enhanced by the chance of choosing from either completing the questionnaire or answering the interview.

The triangulation approach is very appropriate as it allows the researcher to double-check the findings obtained through questionnaires via those collected through the interviews to enhance generalizability and validity. Furthermore, the use of triangulation in this study enriches acceptability of the respondents, reliability of responses, and the quality of the results; thereby boosting the understanding of prevention and detection of electronic banking fraud.

Losee (1993) examined the reasoning method called the deductive approach, which includes the development of theories or concepts that are tested against observation. The

inductive approach is the opposite of the deductive approach. This study employed both inductive and deductive approaches, which is known as an addictive approach, based on the nature of the research objective. For instance, the questionnaire adopted comprised directly related and different questions about the same phenomenon to relate and compare the data collected. The questionnaire employed in this study created certain spaces or gaps in the respondents' comments; hence, it provided a triangulation approach of data collection strategy (Olsen, 2004).

In addition, this study engages with both questionnaires and face-to-face interviews to collect data. The use of both approaches enhances the study's reliability due to the independence of the observers, the higher number of participants, despondences' independence, and opportunity to appraise facts qualitatively and quantitatively (Easterby-Smith et al., 2002). Evaluation and comparison through the adoption of many methods will improve control and accuracy of the research outcomes or findings. The study adopted methodological triangulation because of its strong association with the term "multi-technique appraisal" (in this case, qualitative and quantitative methods).

All factors such as the independence of the respondents and the observers, involvement of many participants, the opportunity of quantitative and qualitative evaluation of facts, the quality of data collected, and comprehensiveness of the resulting analysis resulted in the adoption of mixed methods; in this study, face-to-face interviews and a questionnaire would be the best options (Palmerino, 1999; Easterby-Smith et al., 2002). This is in line with Greene (2008) argument that mixed methods give the opportunity of thinking and generating questions in line with possible answers or results that are jagged and smooth: complete relative certainties in conjunction with possibilities and surprises.

Equally, Denscombe (2007) posited that quantitative and qualitative peculiarity tends to oversimplify issues. Despite the fact they are convenient and appropriate terms to adopt and understand, a perfect distinction between quantitative and qualitative approaches is hard to withstand either at a philosophical or a practical level (Coxon, 2005; Halfpenny, 1997; Hammersley, 1996).

4.5 Research Design

The research strategy for this study is acknowledged as a mixed research technique. This technique comprises the combination of quantitative and qualitative research methods. The use of a mixed research method will make the findings to produce exceedingly reliable results (Creswell et al., 2003; Amaratunga, et al. 2002). The mixed research method is proposed to produce a reliable research method that would lessen the individual feebleness of quantitative and qualitative research. The qualitative research is habitually believed that is susceptible to the bias, confusing in interpretation and weak or inadequate for discovering findings (Creswell, 2009).

In contrast, quantitative research method can be unreasonably miss critical issues in the process of research because of the researcher's perspective, as it disallows other input or additional ideas from the respondents to be investigated. Therefore, the mixed research methods of quantitative and qualitative research techniques can significantly enhance research which attributable to the combination of both techniques that permit the researchers to accept other data while simultaneously sustaining the statistical accuracy of the quantitative method (Creswell et al., 2003). This permits for a wide-ranging research process. The mixed research method is not deprived of its own drawbacks, even though it enhances the sense of balance of the feebleness of each of these amalgamated research approaches. One downside are the challenges entangled in relating the outcomes of both the quantitative and the qualitative research techniques is a single research study.

Finally, the mixed method research study sometimes can be compounded with the requirement of more time and other resources to finish the research successfully. The mixed methods approach was considered to produce both the statistical balance of quantitative methods and an extensive range of understanding and thoughtfulness about the research issues. It was also chosen to escape from difficulties included in both the quantitative and qualitative research approaches. Neither quantitative nor qualitative research approach was satisfactory for full acceptability for the research questions; therefore, the research would be most properly performed using the mixed methods approach.

In addition, to resolve the problem of integrating and announcing the results of the research, the triangulation analysis approach was adopted. Johnson (2008) posited that adopting a pluralist or a pragmatic position assists in advancing debate among researchers from diverse paradigms as they try to develop knowledge and to improve understanding of how research approaches can be successfully combined.

4.6 Population

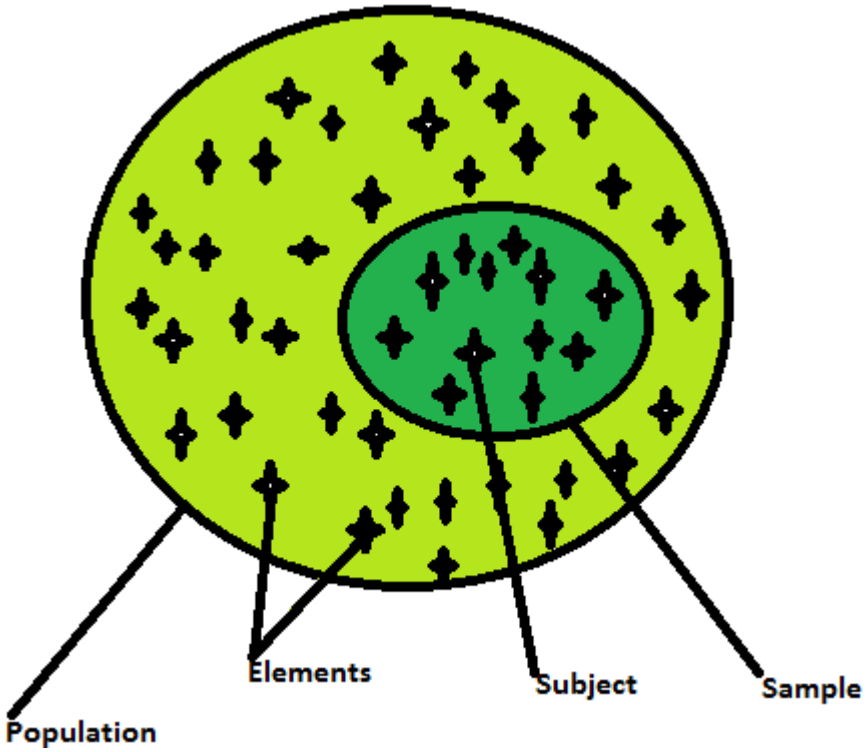
As stated in chapter 2, the Nigerian banking industry made-up of 28 banks, which comprised of 22 deposit money banks (DMBs) that was previously known as commercial banks, 5 merchant banks and 1 non-interest-bearing bank (CBN, 2018). However, the Nigerian deposit money banks, is comprised of 22 banks of 3978 branches all over Nigeria. Hold 78% of the capital reserves, total net assets and also, share over 83% of total profitability in the banking sector, while the remaining 22% of the capital reserve and total net asset, including 17% of the total profitability in the banking sector are shared by the other 6 banks (5 merchant banks and 1 non-interest-bearing bank) (Bank Supervision Report, 2016).

Therefore, the population for this study is mainly entire staff and customers of Deposit Money Banks (MDBs) in Nigeria, which formerly referred to as Nigerian Commercial Banks (NCBs). The choice of the Deposit Money bank based on its highest number of banks (22 banks) and its highest number of branches (3978 branches) all over Nigeria and hold 78% of the total capital that are available in Nigeria. Though, Omotayo, and Kulatunga (2015) observed that, in most case, interviewing the entire population is very difficult, due to inadequate time, limited accessibility, lack of enough funds and other inconveniences. Thus, in this situation, for economic reasons, it will be very easy to interview a subgroup of the population, which means a “sample”.

To get appropriate general conclusions the right or appropriate sample must be selected, hence the sample for this study was selected from 22 deposit money banks which consist of 3979 branches all over Nigeria. It included staff from senior level to the managerial level and customers that have been the victims of electronic banking system within the

bank premises. Sampling enables accessing of every subject of the sample and using the result of the sample collected to make a general conclusion on the intended population.

Figure 4.2: Population, Elements, Sample and Subject



The population for this research is made up of these categories: directors, managers, accounting practitioners and senior staff in internet commerce departments, information technology departments and risk management departments that are working in the head offices of Nigerian deposit money banks. It also included bank customers within the bank premises; customers within the bank premises being considered as victims of e-banking frauds. The categories of the population considered were found to be appropriate because of their heavy participation and involvement in internet banking and online commerce. The participants from the departments were chosen based on their knowledge and level of experience in the subject matter, which would enhance the reliability of the responses for the research instrument based on the research hypotheses.

4.7 Sampling Strategy

There are two categories of sampling methods, namely the non-probability sampling technique and the probability sampling technique. However, if it is essential for the researcher to take a broad view of a widespread population, probability sampling would be the most suitable. Therefore, in the probability sampling technique, the elements or units or people selected as the sample will represent the entire population in the study, permitting generalizations to be conducted, while in the non-probability sampling technique, the selected sample may perhaps not be the best representation of the entire population.

However, it is obvious and popularly accepted that the selection of any sampling method is determined by the research objectives or questions of the study (Dionco-Adetayo, 2011, p. 129; Polonsky & Waller, 2005). It is better for researchers to employ a probability sampling technique where there is the opportunity to do so as it is considered to produce confirmable correct outcomes compared with the non-probability sampling technique. However, there are aspects of research studies which may make it impossible to employ a probability sampling technique. Guba and Lincoln (1994) pronounced non-probability sampling as presence, progressive and emergent. This begins from the types or kinds of the research, development and method, which describes a procedure of finding as contrary to the testing of hypothesis.

The non-probability sampling technique would be appropriate for this study, in which the research questions do not stipulate or require the unit of analysis, for instance a category of people or elements, that should be sampled (Bryman, 2004). Therefore, in this study non-probability sampling, precisely purposive sampling, which also known as Judgement sampling was employed to select the samples or respondents. In any case, most qualitative research lean towards non-probability rather than a probability or random sampling (Saunders, Lewis, & Thornhill, 2015). It has also been suggested that purposive sampling can be adopted when one likes to choose cases or elements that are predominantly informative (Neuman & Neuman, 2000). This means that purposive sampling is employed when there is need to obtain information from a targeted group – that is,

desirable information – because it is the only source where the needed information can be found through certain criteria set by the researcher. Therefore, the non-probability sampling technique empowers the researcher to choose research samples or respondents that have the required experience to understand and discuss the phenomena.

The purposive sampling technique is a non-probability method which permits a sample to be selected from the intended population (Horn, 2010). Purposive sampling is also known as convenience or judgmental sampling as there is no precise sample size (Kemper et al, 2010; Tongce, 2007). Moreover, purposive sampling is employed when populations possess common elements; where a sample describes the entire population, there is a prerequisite for a quota drawn from a larger population with variety, critical cases and peculiar issues, if that is only sampling technique to fit the situation (Bernard, 2006). At pretesting, preliminary and proposal level, there is justification for a study which requires the use of purposive sampling (Wilmot, 2005). Above and beyond, the population from which the sample is purposively selected like expertise, unusual skills, and knowledge of specific facts (Barratt, Ferris & Lenton, 2015; Kothari,2004).

Each time a fraud incident occurs, there is a victim and a perpetrator. It would have been better to gather opinions and views from fraud perpetrators to get a better picture of their motivations for committing frauds. However, looking for fraudsters to interview or to administer questionnaires to, would have been a complicated issue. The fraudsters would undoubtedly be less likely to give straightforward and truthful information on their motivations and activities.

Therefore, collection of the information about e-banking fraud prevention and detection in banking industry required people that are well-informed, educated and conversant with e-banking fraud incidences in the banking sector. In the same vein, Paler-Calmorin (2007) opined that the use of a mechanism for fraud detection and prevention is decided at the directorial, structural or administrative level of the organization. Also, Krambia-Kapardis (2002) argued that when investigating corporate losses from fraud, it is important to choose suitable participants in the institution to be investigated; failing to do this may result in a low response rate. The selection of whom to speak with, when, where, about

what, and why, places limitations on the conclusions drawn and the degree of confidence others can have about the outcome (Miles & Hubermann, 1994).

In a nutshell, with the above reasons and the nature of e-banking fraud prevention and detection, purposive sampling, which also known as a judgement sampling technique was employed for selection of both respondents of quantitative research and participants in qualitative research. Hence this study sampled accounting practitioners, professional bankers, directors and managers, because this research is actually focused on the decision-making process, which is the major managerial responsibility of the chief financial officers, chief accountants, directors and managers; including the heads of internet banking, heads of fraud investigation, heads of information systems and technology, heads of operational risk management, heads of internal audit units, heads of security personnel, heads of forensic audit, heads of financial crime team members, and others. These staff are in the best position to provide the needed information. Also, customers from the banking premises where selected for the second face of the questionnaire. The selection of the customers was based on those who had previously been the victims of fraud. This would certainly contribute to enhance the reliability of the data obtained.

4.8 Sampling and Sample Size

Works on the sampling method state that a specific sample frame is important for random sampling. According to Tran and Perry (2003), non-probability sampling is employed in research when it is the only feasible and viable option to adopt in the aspect of restrictions in selecting probability sampling; therefore, the choice of non-probability sampling requires solid assumptions on the nature and proportion of the sample for its validity.

For both the qualitative research and quantitative research questions used to examine electronic banking fraud detection and prevention in Nigerian banks, 10 deposit money banks (MDB) in Lagos and Abuja out of 22 deposit money banks in Nigeria (CBN, 2017) were selected as a unit of the population, using a purposive sampling technique. Directed by the above arguments, only ten deposit money banks in Nigeria (given anonymous

titles: Bank A, Bank B, Bank C, Bank D, Bank E, Bank F, Bank G, Bank H, Bank I and Bank J) were chosen as the representative sample from the sample frame.

Firstly, the rationale for selecting ten deposit money banks in Nigeria from the 22 banks with 3979 branches (CBN, 2017) that were available in the Nigerian banking sector was that, the selected 10 deposit money banks in Lagos State and Abuja Federal Capital Territory (FCT) had 2902 branches which made- up 73% of all bank branches over the 36 states of Nigeria, while the other deposit money banks had only 1077 branches, making up 27% of the total (CBN, 2017). The selected banks were appropriate because of their heavy participation and involvement in electronic banking and commerce.

Secondly, the choice of Lagos as the main place of this study was to do with the number of head offices of deposit money banks in Lagos. Out of 22 banks in Nigeria, 21 head offices were in Lagos while the remaining one located in Abuja. Thus, the choice of these banks based on the number of the branches owned by each of the banks, geographical location and their proximity to one another were also considered. Ten banks that have the highest number of branches all over the country were selected (CBN, 2017). Precisely, the head offices of 9 banks were selected while only 1 bank in Abuja which is the second bank with the highest branches in Nigeria also selected. Therefore, the selected banks are the banks that have the greatest numbers of branch offices and staff across the country; this gave opportunities to capture the needed information on the subject matter from every nook and cranny of the country.

Information generated through qualitative and quantitative research was adopted for this study. This study employs the idea posited by Creswell et al. (2003) on the method for chronological exploratory strategy; that is, the quantitative and qualitative approach (QUAN QUAL approach), as this method gives opportunity to collect data through face-to-face qualitative interviews after the responses have been collected from the quantitative survey. The qualitative interviews were adopted to investigate further the results obtained from the questionnaire data. This supported interview carried out with ten selected top managers from the selected Nigerian deposit money banks through a purposive sampling technique, with at least one head for each of the following

departments: Application and Database Security Management, Frauds and Risks Management, and Fraud Control and Monitoring Management. The participants who had answered the questionnaire were excluded from participating in the interviews to escape positive bias. The main reasons for the use of qualitative interviews were to enhance the understanding and to elucidate the quantitative results.

Moreover, for the quantitative research, representative samples were sourced from two groups with two different classes of questionnaires. The first group comprised the representative of banks' staff as experts in banking business. A sample size of 383 was initially determined out of estimated 113,200 bank staff in Nigeria. While, the second group comprised the representative of banks' customers as victims of e-banking fraud with a sample size of 384 out of the estimated 22 million bank customers in Nigeria was also originally determined with the use of an online electronic sample calculator for a 5% confidence interval and 95% confidence. However, there are two classifications of sample size generally recommended in factor analysis (EFA and CFA). The first group agreed that the complete number of samples (*N*) is significant, while the second agreed that the subject-to-variable ratio (*p*) is imperative (Velicer, Eaton & Fava 2000; Velicer & Fava, 1998; Arrindell & van der Ende, 1985, and MacCallum, et al., 1997). A minimum sample of 100 is appropriate, that it is, the sample size should not less than 100 samples for factor analysis, even though the variable size is not up to 20 (Gorsuch, 1974; Psylch & Hatvher 2013; Arrindell & Van der Ende, 1985). , Hatcher (1994) and David Garson, 2008) also suggested 100 samples as minimum sample size for a factor analysis while, Hutcheson and Sofroniou (1999) acclaimed at least 100 – 200 samples as a moderate sample size.

In addition, many scholars have used a ratio 10:1 of subjects-to-variables in their studies (Orakci & Toraman, 2018; David Garson, 2008; Nunnally, 1978, Marascuilor & Levin, 1983). A ratio between 3:1 and 6:1 of subjects-to-variables is acceptable if the minimum variables-to-factors ratio 3 to 1. But, the absolute lowest sample size must not be less 100 samples for EFA and CFA (Kline, 2004; Comry & Lee, 2013; Fabriger et al., 1999). Ferguson & Cox (1993), and Marsh and Hocev (1985) opined that sample size use in any

large study must, not less than 100 samples. Therefore, having considered the types of analyses employed (EFA and CFA), the level of accuracy and precision required, population heterogeneity and homogeneity, sampling technique employed (purposive sampling technique) and availability of resources and targeted respondents (bank staff at management level and e-bank fraud victims among the customers within the bank premises). The researcher decided to limit the sample size of the study to 200 samples for each group of staff respondents and customer respondents which their ratios of subject-to-variables range between 5:1 and 10:1.

Hence, the sampling method was to survey all potential respondents and to get their permission for the research's engagement. As it turned out, 169 of the 200 determined questionnaires were returned for the quantitative research on the banks' staff, while 165 out of the determined 200 questionnaires were returned for the quantitative study of the bank's customers. Also, all ten top managers contacted face to face with semi-structured interviews agreed to participate and gave their useful responses. The response rate that would be confirmed as suitable and appropriate representation was anticipated to be between 40% and 50% (Blumberg, Cooper & Schindler, 2005). The qualitative survey gained a 100% response rate, while the quantitative study of the banks' staff achieved an 85% response rate and the survey of the banks' customers gained 78% response rate. Consequently, a high and appropriate response rate was accomplished through self-administration of a simple questionnaire, adequate follow-up, short length of interviews, advance notification of respondents and positive interest of the participants in the research.

4.9 Research Instruments Design and Testing

Primary data were collected through the means of interviews and questionnaires. The questionnaire survey strategy was employed in this study. Extant literature has identified that the questionnaire is the best and the most appropriate instrument for data collection when employing the survey strategy in this kind of business research (Dionco-Adetayo, 2011; Kothari, 2004). Dionco-Adetayo, (2011) argued that the questionnaire is a technique for collecting information. It is a pro-formulated written set of carefully worded

questions and instructions related to a problem for the respondents to answer. Thus, this research used both face-to-face interviews and self-administered questionnaires in order gain understanding of the perspectives of different groups. Consequently, self-administered questionnaire method was adopted as Dionco-Adetayo (2011) has proved that the self-administration method provides an efficient way of collecting data from many respondents and enhances researcher's understanding through self-observation. Hence, this method provides quantitative data analysis that supports the deductive approach to the objectives and the research questions of this study as set out in Sections 1.3.

Furthermore, these questionnaires were in two categories which are questionnaires for the bank staff and questionnaires for the bank customers. The first category was questionnaires for the bank staff, which structured into 5 sections with 97 variables. Section A labelled 'demographic data' has 6 variables. Section B examines 'the current nature of e-banking fraud that are of high concern in Nigerian Banking industry' with 6 variables. Section C, measures 'the factors contributing to the increase of e-banking frauds in Nigerian banks' with 30 variables. Section D measures 'current preventive mechanisms of e-banking fraud in Nigeria banks' with 30 variables. While, section E measures current detective mechanisms of e-banking fraud in Nigeria banks with 25 variables (see Table 4.2). While, the second category was questionnaires for the customers within the selected bank's premises which have 2 sections with 30 variables. Section A labelled 'demographic data' has 3 variables. Section B with 28 variables. It should be noted that response modes and questions in a questionnaire can come in different forms.

Nevertheless, the questions for the questionnaires employed in this study were closed-ended. The respondents were limited to selecting their answers from prearranged options. The type of technique is generally known as forced-responses. Forced-responses means that respondents must answer the questions according to the structured pattern of the questionnaire (Kothari, 2004). In addition, 20 questions were prepared for qualitative survey.

However, excepting demographic attributes which used nominal scaling, all other sections were Likert-scale. It has been debated whether ordinal questions are commonly used with the Likert scale (Singh, 2006; Katheri, 2004 and Dionco-Adetayo, 2011). The Likert scale was developed by a sociologist called Rensis Likert at Michigan University. It was named the "Likert scale" after him in a report titled "A Measurement of Attitude's Techniques" that was published in the Psychology Archives in 1932. His aim was to develop a way of measuring psychological attitudes in a scientific manner (James & Thomas, 1990). Dionco-Adetayo, (2011) explained the Likert scale as bi-polar, which means that it starts from positive through neutral to negative.

Specifically, the Likert scale is in the following format: Strongly Agreed 5, Agreed 4, Undecided 3, Disagreed 2, Strongly Disagreed 1. However, there are different names given to the varying states depending on the kind of rating individual researcher preferred (Brown, 2010). For the benefit of this study, the researcher maintained the original format by assigning scores from 5 to 1 from positive to undecided options. Thus the five-point Likert scale is adopted for this study, which bears the following rates: Strongly Agreed 5, Agreed 4, Undecided 3, Disagreed 2, Strongly Disagreed 1 (Appendixes 2 & 3). Moreover, the drafting of questionnaire was done with caution to follow the process and the procedures of translating constructs into meaningful and acceptable words. The words used were considered when the understanding of the respondents had been put as a priority. In designing the questionnaire, a lot of effort was put into selecting appropriate words to avoid leaving room for misunderstanding and misconstruction. It is necessary to design a questionnaire in such a way that it will be easy for the respondents to answer conveniently.

Frazer and Lawley (2000) posited that neutral, appropriate and relevant questions improve the accuracy of responses from the respondents. Also, to gather appropriate and valuable data from the respondents, a closed-ended questionnaire was adopted, since this is the best category of questionnaire format that is available for this nature of the research question. The questions were structured and made attractive in a manner that motivated and did not impede the respondents from answering the questions. The questionnaire was

carefully designed and well presented to escape the confusion and ambiguity (see the Table 4.2 and Appendix 1b).

Additionally, for the benefit of validity, the ideas of the questions for both quantitative and qualitative questions were sourced from the study titled "India Banking Fraud Survey" (Deliotte, 2015). Also, the researcher sought expert advice and guidance from a team of selected professional accountants and academics from the department. Piloting and pre-testing questionnaire are vital processes that need to be gone through in order to be sure that the questionnaire is free from any potential mistake or problem and to present clear and easily understood questions with an appropriate time phase for completion and recovery of feedback that meets the exact expected aim. The feedback from the pilot run may call for questionnaire adjustment as many times as possible.

Therefore, the pilot of this study was done between on the 19th and 23rd December 2016 through testing of the questionnaire by a group of people from the intended respondents for the main study to discover the likely deficiencies in the questionnaire design and its administration. Out of the ten Nigerian deposit money banks selected for the main study, five were chosen for the pilot. The questionnaires were distributed to 25 staff respondents working as managers, accountants, internal control staff and internal auditors in the selected Nigerian deposit money banks and 10 customers respondents (see Table 4.21).

Table 4.1: Pilot Questionnaires Administered and Returned

Pilot Questionnaires Administered and Returned				
Nigerian deposit money banks	Number of Quest.		Number of Quest.	
	Distributed		Returned	
	Staff	Customers	Staff	Customers
United Bank for Africa	5	2	5	2
First Bank of Nigeria plc	5	2	5	2
Zenith Bank Nigeria plc	5	2	5	2
Skye Bank Nigeria plc	5	2	5	2
Access Bank plc	5	2	5	2
	25	**10**	**25**	**10**

The pilot survey questionnaire was accompanied by a covering note or letter to each of the respondents which described the primary aims of the study and gave assurance of the confidentiality and anonymity of the data supplied in the pilot questionnaire. Also attached was a guideline for completing the questionnaire.

Table 4.2: Analysis of the Pilot Quantitative and Qualitative Questions

Section	Research Pilot Question Titles	No of the Items of Questions
A	Demographic Data	6
B	The e-banking fraud risks that are of high concern in	6
	the Nigerian banking sector	
C	The perceived factors that have considerable	30
	influence on the increase in e-banking fraud in Nigeria	
D	The current significant mechanisms for e-banking fraud	30
	prevention in the Nigerian banking industry	
E	The current significant mechanisms for e-banking	25
	fraud detection in the Nigerian banking industry	
Total		97
BC	Customers Awareness of E-banking Frauds in Nig. Banks	22
QU.	Qualitative (Interview Questions)	10

Moreover, almost all respondents to the pilot questionnaires and qualitative questions commented that both the questionnaires (97 questions) and the interviews (20 questions) included questions for the customers (30 questions) consumed a lot of time to complete. Some respondents suggested that some questions should be merged into one question, particularly, the related questions that produced almost the same answer, one should be chosen, and the others should be deleted. All the comments were painstakingly considered accordingly. Therefore, the questionnaire's questions for the staff were reduced to 87 questions (see Appendix 2) and the total number of interview questions to 10 (see Appendix 4). While, the questionnaire for the customers also was reduced to 22 questions (see Table 4.2 and Appendix 3). The following table shows the analysis of the staff questionnaire and interview.

Table 4.3: Analysis of the Quantitative and Qualitative Question

Section	Research Question Titles	No of the Items of Questions
A	Demographic Data	6
B	The e-banking fraud risks that are of high concern in the Nigerian banking sector	6
C	The perceived factors that have considerable influence on the increase in e-banking fraud in Nigeria	28
D	The current significant mechanisms for e-banking fraud prevention in the Nigerian banking industry	27
E	The current significant mechanisms for e-banking fraud detection in the Nigerian banking industry	20
Total		87
BC	Customers Awareness of E-banking Frauds in Nig. Banks	22
QU.	Qualitative (Interview Questions)	10

The interview questions were split into two groups of four; Group A was for five interviewees in the first five selected deposit money banks and Group B for five interviewees in the other five selected deposit money banks. Due to the outcome of the pilot, the questionnaire was adjusted to enhance the reliability and internal validity of the technique for collection of high-quality and useful data for the research study.

4.10 Data Collection Procedure

The researcher seeks for the permission of the respondents through telephone calls and letter of consent sent to the selected banks before, the interview and questionnaire administration period, which supported face to face interview with the aid of a tape recorder and taking of notes, and self-administration of questionnaires which took place between on the 14th April and 26th May 2017. These methods gave the researcher a perfect access into the headquarters of the selected banks located in both Lagos state and Abuja. Nevertheless, gaining access to the individual questionnaire respondents and interview participants was very hard, but through management and personal interaction connections with the respondents and participants the aims were achieved.

Moreover, before the interview with the staff or participants, the researcher introduced himself. After the greeting, the introduction of the researcher's educational background and current university with the programme of study was formally done; the explanation of the purpose of the data collection, which is purely academic was made clear to the respondents, and also, to comply with ethics, the respondents were informed that, if at any stage they wished to withdraw from the exercise, they were at liberty to do so. Nevertheless, the researcher solicited for the respondents to stay to the end and all the staff made themselves available to help. While, a copy of the letter of introduction was attached to each of the questionnaires administered to both the staff and the customer respondents.

Furthermore, with the help of bank manager, the customers in the bank premises were asked that, if any, customer had been a victim of fraud, particularly e-banking fraud should signify themselves and those that complied were asked to come out to where the researcher introduced himself in the analogous way as above and the questionnaires were distributed to the interested customers.

4.11 Data Preparation and Analysis Procedure

Several authors have argued that quantitative data should be screened, edited, coded, reformed and inputted into a database before it can be analysed and interpreted (Hair et al, 2010; Crowther & Lancaster, 2009; Sekaran & Bougie, 2010; Hair et al., 2007; Lancaster, 2005). However, there is no specific agreement on which process and pattern it should take. In this research work, preliminary checking of the retrieved questionnaire was carried out to inspect for invalid and valid responses.

4.11.1 Data Preparation

The Statistical Package for the Social Sciences (SPSS) was employed and the variables in the questionnaire were coded and named to correspond with the variable coding instructions and variable names in SPSS to be able to track the variables in the survey questionnaires and to examine the manner they are described in the SPSS data base.

Having collected the data, the researcher began the sorting, editing, and coding of the data. The data collected through interviews were analysed based on the arguments, views and explanations of the participants. With the help of SPSS, the data gathered through the administered questionnaires were analysed through both descriptive and inferential statistics.

Table 4.4 Statistical & Analytical Tools Employed

S/N	Research Propositions	Techniques
A	The e-banking fraud risks that are of high	Freq. Analysis
	concern in the Nigerian banking sector	
B	The perceived factors that have considerable.	Freq. Analysis,
	influence on the increase in e-banking fraud in Nigeria	EFA & CFA
C	The current significant mechanisms for e-banking	Freq. Analysis,
	fraud prevention in the Nigerian banking industry	EFA & CFA
D	The current significant mechanisms for e-banking	Freq. Analysis,
	fraud detection in the Nigerian banking industry	EFA & CFA
BC	Customers awareness of e-banking fruad	Freq. Analsys

Moreover, the bivariate analysis was empowered by a non-parametric technique for measuring linear association between the variables based on ordinal datasets (Pallant, 2013). Pie charts, bar charts and frequency tables were used to summarize, group and show the output of the administered questionnaires four distinct categories which applied to analyse all quantitative research questions included customer's responses while cross-tabulations analyses were applied to explore the direction and strength of the relationships between the variables generated by the frequency tables of demographic data of this study. The cross-tabulations immensely contributed to the analysis of this study's data precisely, demographic data, in relations to the direction of the relationships.

In short, this descriptive statistical analysis was used to analyse all quantitative questions while, inferential statistical analysis was employed to analyse the responses to research

questions 2, 3 and 4. Meanwhile, the responses to the interview questions were analysed with the use of thematic analysis which explained in chapter six.

Correspondingly, as said earlier, two statistical techniques were employed to analyse the quantitative data: descriptive statistics and inferential statistics. Descriptive statistics were used to summarize and recapitulate to acquire better advance understanding of the data set. This was carried out for all classes of data to present their general trends with the use of frequency distributions of measures of central tendency with the aid of pie charts and bar charts to display the frequency distribution. Inferential statistics were applied to the view of testing the hypotheses formed for this study through the research questions stated in the section 1.3.

Furthermore, inferential statistical technique employed for the data analyses and for the testing of hypotheses from research questions 2,3 and 4 only. This inferential statistical technique employed is parametric tests.

Parametric tests rest on the physiognomies and attributes of the population for their use, if the data have equal variance and are normally distributed (Udofia, 2011, Ho, 2006, p. 357). Non-parametric tests make fewer assumptions about the population; henceforth they are referred to as “distribution-free”. Therefore, the parametric tests were employed in this study using the exploratory factor analysis and the structural equation modelling (SEM). The reasons and the procedures for the adoption of these statistical techniques are given below.

4.11.2 Factor Analysis

Factor analysis was employed to answer question 2, which seeks to identify the contemporary perceived factors that have considerable influence on the increase in e-banking fraud in Nigeria; Research question 3 and 4, which seeks to recognize the current mechanisms of prevention and detection of e-banking fraud in Nigeria; and to answer related research questions (see Section 1.3). The purpose of factor analysis is the method simplification of many interrelated measures or components into a small number of representative factors or constructs (Ho, 2006). A researcher may choose to perform

factor analysis as either as R- mode or Q-mode. The R-mode deals with the columns, resulting in a minimization in the number of variables of observations, while Q-mode factor analysis deals with the rows, leading to a reduction in the number of observed variations. It is argued by scholars that R-mode factor analysis is more generally accepted, since many researchers are concerned with minimizing the number or total of variables in any given research situation (Miesch, 1975; Udofia, 2011).

Factor analysis assists a researcher minimizing a large volume of variables. In factor analysis, it is presumed that entire variables are correlated or interrelated to some level or degree. It is thus assumed that variables with comparable or parallel dimensions should be highly correlated while those with different dimensions would have low correlation. Therefore, in the correlation matrix, these low- and high-correlation coefficients become obvious as variables with related dimensions that are interrelated or correlated (Ho, 2006, p 203).

Three main steps are necessary in factor analysis (Raykov & Penev, 2001; Ho, 2006; Udofia, 2011). These are the computation of the correlation matrix, extraction of the initial factor loadings, and rotation of extracting factors. In the computation of the correlation matrix, intercorrelation coefficients of variables were computed, which was followed by the extraction of initial factors with the use of SPSS Version 23 software. There are two main techniques for extracting initial factors: common factor analysis and principal components analysis. The SPSS program further provides an additional six techniques under common factor analysis (Pallant,2001). The principal component analysis (PCA) method was suitable and appropriate for this study, since it is designed for data reduction to attain a small number of constructs or factors to represent the original data set (Holland, 2008). Therefore, in this study, to select the appropriate and suitable loaded factors with the use of PCA the following techniques

4.11.2.1 Correlation Matrix

Loaded factor to be satisfactorily interpreted, it is important to evaluate the appropriateness of the data for factor analysis. One method of performing this is to

visually examine the magnitude of factor loadings on the correlation matrix, such as correlation coefficients between the factors and the variables they represent. Factors with correlation coefficients greater than 0.33 (i.e. Approximately 10% of the total variance in the variable is described by the factors) were accepted and considered noteworthy and significant; those with lesser values may not yield interpretable and acceptable factors (Pallant, 2007).

4.11.2.2 Bartlett's Test of Sphericity

Another technique for evaluating the appropriateness and suitability of the data set for factor analysis is by computation of Bartlett's test of sphericity (Willians, Onsma & Brown, 2010) and the Kaiser-Mayer-Olkin (KMO) measure of sample statistics (Pallant, 2005; Batlett,1950). Pallant (2010) opines that the KMO index (extending between 0 and 1) ought to be at least 0.6 for satisfactory and suitable factor analysis, while the Bartlett's test ought to be significant at 0.05 ($p < 0.05$) which were also considered in this study.

4.11.2.3 Eigenvalue

Eigenvalue reflects the number of extracted factors, which is equal to the number of items that are accounted for in factor analysis. The number of the initial loading factors to be retained and rotated or extracted can be ascertained by three conventional approaches: eigenvalues, scree plot test criteria and parallel analysis. The eigenvalue is the ratio between the common variance and unique variance explained by exact factors extracted (Pallant, 2010). With the eigenvalue principle, only factors with an eigenvalue of 1 and above are considered significant while those less than 1 are disregarded. Therefore, eigenvalue was employed to select the loaded latent factors used in this study.

4.11.2.4 Scree Plot

Scree plot is a line graph of the eigenvalues of all the factors. This line graph is suitable for determining the number of factors to retain. The scree plot test is used to recognize the maximum number of factors that can be extracted before the total of unique variance starts to dominate the common variance structure (Hair et al., 2007). If the numbers of

extracting factors on the x-axis are plotted in order against eigenvalues on the y-axis, then a scree plot test ensues. The scree plot is shown in a graphical form as a steep slope between the initial large factors and the gradual tailing off the rest of the factors. The minimum number of factors to be retained is specified at the point of inflection of the curve. In summary, the factors above the inflection are retained and considered useful while those below are not. Therefore, scree plot was used to support eigenvalues in the selection of the loaded factors in this study.

4.11.2.5 Parallel Analysis

Parallel analysis was equally adopted to determine the number of factors to retain out of the factors with an eigenvalue greater than 1(Ledesma & Valero-Mora, 2007). Systematically, the first eigenvalue obtained from principal component analysis (PCA) in SPSS was compared with the equivalent first result from the random values obtained from parallel analysis. The factor was retained if the eigenvalue from principal component analysis (PCA) in SPSS was greater than the criterion result from parallel analysis; if it was otherwise, the factor was rejected (Hayton, Allen & Scarpello, 2004; Willianms, Onsman & Brown, 2010). In this study, these criteria were adopted in determining the numbers of factors to be extracted.

4.11.2.6 Rotation Component Matrix

The initial factors are always difficult to interpret; thus, there is a need for rotation of the extracted factors (Pallant, 2005). The rotation component matrix does not essentially change anything but eases the interpretation of the analysis (Ulbrich et al., 2009). There are two approaches: oblique and orthogonal (Udofia, 2011; Ho, 2006). The orthogonal rotation approach maintains the reference axes of the factors at 90º if the factors are independent, while the oblique rotation approach maintains correlated factors at the level of independence amongst the rotated factors. In view of this, the existing study adopts orthogonal rotation. Scholars have debated three major approaches of orthogonal rotation: varimax, quartimax and equimax (Ho, 2006; Udofia, 2011; Pallant, 2007). The varimax

rotation was used in this study as it is the method that most commonly used by scholars which seems to give the purest separation of factors (Pallant, 2005; Ho, 2006).

In addition, the factor loadings on the varimax rotated component matrix were observed for substantial cross-loading that fits the interpretation of output. Investigation of the factor loadings proved that most of the variables were highly loaded on the first factor (Pallant, 2005; Williams, Onsman & Brown, 2010; Olawale & Garwe, 2010). However, Kiolbassa et al., (2011) suggests possible ways to handle this by evaluating the wording of the cross-loaded variables and, grounded on their face validity, allocating them to the factors that are most logically or conceptually representative, and, thereafter, naming the factors. Finally, factor analysis was adopted to categorize the factors of e-banking fraud increase and e-banking fraud prevention and detection mechanisms, because of the sample size (200), which is large enough and there was appropriate significant correlation in the data matrix. This was further processed using structural equation modelling (SEM).

4.11.3 Confirmatory Factor Analysis (CFA)

Confirmatory Factor Analysis (CFA) is a multivariate co-relational analysis procedure (Schumacker & Lomax, 2004). It was the most appropriate analysis technique adopted in this study for the quantitative analysis specifically to answer question 2, which seeks to identify the perceived factors that have considerable influence on the increase in e-banking fraud in Nigeria and also, research question 3 and 4, which seeks to recognize the current mechanisms of prevention and detection of e-banking fraud in Nigeria; and to answer related research hypotheses (see 1.2). Because CFA is a statistical analysis tool for testing the theoretical relationship between the observed and latent variables. It involves the mixture of factor and regression analyses (Tabachnick & Fidell, 2007).

CFA is also known as path analysis technique and is used for multiple correlations and evaluation of relationships, commencing from exploratory analysis to confirmatory analysis (Hair et al., 2010). Structural equation modelling through the structural model estimates multiple simultaneous equations. CFA has been used in similar studies, such as those of Suleiman, et al (2012) and Dimitrios, Dimitrios, and Lazaros (2013). It is,

therefore, despite certain limitations, required for theoretical model and hypothesis testing in the current research.

However, to perform CFA, there is a need for a theoretical model with observed variables and unobserved variables. Therefore, to determine the observed variables, latent or unobserved variable computation of exploratory factor analysis (EFA) was required, and then confirmatory factor analysis (CFA) for construct validity (Brown, 2014). Moreover, the outcome of confirmatory factor analysis produced convincing evidence of theoretical construct differentiation and convergent validities. Discriminate validity indicated that there was no high intercorrelation among the diverse indicators of theoretical constructs, while convergent validity meant that there was overlapping or interrelation between various indicators of the theoretical constructs (Schumacker & Lomax, 2004).

Subsequently, hypothetical models were computerized to identify the collaboration between the factors produced by exploratory factor analysis (EFA) and thereafter to determine the extent to which the theoretical model was supported by the sample data using Amos (Schumacker & Lomax, 2004). Moreover, the hypothetical model was modified through the strict observation of fit indexes and significance values: certain factors were removed from the hypothetical model due to their feeble association and correlation with other factors. A modified model with acceptable or excellent fit indexes that significantly and plausible associations among the constructs was fitted and identified as the model.

In this study, identification of the model fit was done by first examining the statistical significance of the parameter estimates of the path, which is commonly appraised by the 0.05 level of significance (Schumacker & Lomax 2004). The next standard considered was an examination of the fit indexes, such as the chi-square (χ^2), Tucker-Lewis index (TLI), comparative fit index (CFI), and root mean square error of approximation (RMSEA). In the Amos fit, measure, there are three estimated techniques that are usually used to compute the χ^2 *statistic* in unmeasured-variable or latent-variable models: maximum likelihood (ML), unweighted least squares (ULS) and generalized least squares (GLS). Each method estimates the model fit and evaluates a best-fitting result. Loehlin

(1987) opined that the ULS estimate does not rely on an assumption of normal distribution; therefore, its estimates are inefficient and scale variant, unlike ML and GLS.

Maximum likelihood (ML) evaluations are unbiased, dependable, scale invariant, efficient, normally distributed and scale-free if the measured variables match with the multivariate normality assumption. Generalized least squares (GLS) valuations have comparable properties to the ML technique under a low rigorous multivariate normality assumption and make available an estimated chi-square test of model fit to the data. However, the researcher has chosen the ML chi-square estimation method for the model analysis in this study.

Model fit (MF) of the maximum likelihood is used to evaluate the degree to which the sample variance-covariance data fit the structural equation model. The normally used measures of model fit include chi-square (χ^2), adjusted goodness-of-fit index (AGFI), goodness-of-fit index (GFI) and root-mean-square residual (RMR) with the Amos program. These measurement techniques are based on variances between the model-implied variance-covariance matrix and the measured samples; hence, these models fit the criteria. Chi-square (χ^2), the adjusted goodness-of-fit index (AGFI), the goodness-of-fit index (GFI) and the root-mean-square residual (RMR) were adopted as appropriate for this study.

The likelihood ratio chi-square (χ^2) statistic is an essential indicator and major statistical measure of the overall goodness-of-fit used in structural equation modelling (Schumacker & Lomax, 2004). When using the chi-square test, the researcher usually aims to reject the null hypothesis and accept its alternative, particularly when there is a statistically significant variance between the “expected” and the “observed”; therefore, the higher the chi-square the better it fits. However, it is otherwise in structural modelling: there the researcher is interested in getting insignificant variances with related degrees of freedom between the predicted and the actual matrices (Wothke, 2000).

In structural modelling, the researcher is interested in accepting or not rejecting the null hypothesis; thus, the lower the chi-square the better the fit of the sample variance-covariance data. The chi-square is sensitive to withdrawals from multivariate normality

in measured variables, indicators and intensifies as a main purpose of sample size. Schumacker and Lomax (2004) posited that the χ^2 statistic of model fit may lead to inaccurate decisions concerning analysis of outputs. The chi-square model of the fit measure is delicate to observed sample proportion as the observed sample proportion rises (specifically, equal or greater than 150), the chi-square measure has a propensity to show a significant probability rate. In contrast, as sample proportion declines (specifically, below 100), the chi-square measure displays insignificant probability levels (Blunch, 2012). Hence, χ^2 is influenced by sample proportions, due to its computation from $\chi^2 = (n - 1) fq$, where fq is the maximum likelihood fit function.

The goodness-of-fit index (GFI) is determined by the ratio of the addition of the squared variations between the original covariance matrix and replicated matrices to the measured variables. The GFI evaluates the value, variance and covariance in the original covariance matrix that is forecast by the reproduced (implied) covariance matrix based on a factor model (Blunch, 2012). The GFI is an examination of the degree of model fit associated with a single model (no model) (Schumacker & Lomax, 2004; Blunch, 2012; Ho, 2006). The GFI model fit criterion ranges from 0, signifying no fit, to 1, representing an excellent fit. Specifically, a value close to 0.95 shows a good fit (Schumacker & Lomax, 2004; Blunch, 2012). The adjusted goodness-of-fit index (AGFI) is attuned from the degrees of freedom (DF) of a specific model compared to a certain number of variables. The AGFI is calculated as $1 - [(R/DF)(1 - GFI)]$, where R represents the number of single distinct values in the original covariance matrix, $p(p + 1)/2$, and DF is the number of degrees of freedom in the model. The model fit scale for AGFI runs from 0 (no fit) to 1 (excellent fit). Specifically, an AGFI of 0.95 indicates a good model fit (Schumacker & Lomax, 2004; Blunch, 2012).

The RMR index employs the square root of the mean squared variances between the observed and implied covariance matrices. In other words, it is the square root of the inconsistency between the model covariance matrix and the sample covariance matrix. The root means square error of approximation (RMSEA) evades issues of sample size by investigating the variation between the hypothesized model and the optimally selected

population covariance matrix and parameter estimates. The RMSEA is scaled from 0 to 1, with lesser values representing better model fit. A value of 0.05 or less signifies satisfactory model fit (Schumacker & Lomax, 2004; Blunch, 2012). Despite the role of the chi-square of the model fit of unobserved variable models, another five measurement indices have been developed as variants for relating alternative models: The Tucker-Lewis Index (TLI), normed fit index (NFI), relative fit index (RFI), incremental fit index (IFI) and comparative fit index (CFI). These classically compare a proposed model with an independence model (null model) (Schumacker & Lomax, 2004; Blunch, 2012).

The Tucker-Lewis Index (TLI) is used to equate alternative models or a projected model against a null model. The TLI ranges from 0 (no fit) to 1 (excellent fit). Typically, a value close to 0.95 reflects a good model fit. The value of TLI of this current study was calculated as $[X^2\text{null}/df\text{null}) - (X^2\text{model}/df\text{model})] /[(X^2\text{null}/df\text{null}) - 1]$. The normed fit index (NFI) is used to rescale the chi-square from a no fit (0) to excellent fit (1.0) level (Schumacker & Lomax, 2004). It is measured to assess a constrained model with a completed model by means of baseline null models such as this: $(X^2\text{null} - X^2\text{model}) /X^2\text{null}$. The comparative fit index (CFI) is used to measure the development in the non - centrality in proceeding from the least restrictive model of a saturated model.

The relative fit index (RFI) is calculated by the mean of $RFI = 1 - [(X^2\text{model}/df\text{model}) /(X^2\text{null}/df\text{null})]$, while the incremental fit index (IFI) = $1 - [(X^2\text{null} - X^2\text{model}) /X^2\text{null} - df\text{model})]$. Schumacker and Lomax (2004) and Blunch (2012) posited that a value close to 0.95 reflects a good model fit. (Note: X^2model = the default model, model of the discrepancy; *df*model = the default model, model of degrees of freedom; X^2null = the independence model, model of discrepancy; *df*null = the independence model, model of degrees of freedom). The benchmark for model fit indexes varies in various articles. Hu and Bentler (1999) and Schumacker & Lomax, (2004) elucidated that it is hard to attach a fixed benchmark value to each of the fit indexes because they do not perform correspondingly well in diverse circumstances. Correspondingly, Schumacker and Lomax (2004) stated that there has been much debate on the subjective appropriateness and the independent interpretations of a modelling condition.

However, Hu and Bentler (1999) suggested benchmark measures of 0.95 for fit indexes, while a non-significant measure has been suggested for the chi-square (Schumacker & Lomax, 2004). Notwithstanding this, it has been noted that the chi-square benchmark (non-significant) can be prejudiced by the sample size, particularly if the sample size is above 200. Likewise, Browne and Cudeck (1993) proposed that the benchmark value for the RMSEA index must be less than 0.05, while benchmark values of GFI, AGFI, TLI, NFI and PFI close to 0.95 reflect a good model fit.

4.11.4 Reliability

Tavokol and Dennick (2011) posited a standard rate of reliability for measuring instruments in sample sizes of over 200 with the use of the Cronbach's Alpha formula. A reliability level of 0.90 and above is accepted as strongly reliable, 0.80 to 0.90 is regarded as highly acceptable, 0.70 to 0.80 is regarded as acceptable, 0.60 to 0.70 is regarded as less acceptable, below 0.60 is regarded as unwanted. Therefore, the Cronbach's Alpha Formula was adopted in this study using the SPSS package; it showed the reliability coefficients of the items related to e-banking fraud prevention and detection in the research questionnaire to be at levels between 0.70 and 0.99.

4.11.5 Validity

Samples of 200 staff and 200 customers were selected from deposit money banks in Nigeria as descriptive and inferential tests of structural equation modelling (SEM) are more reliable with a large sample. Discriminate validity and convergent validity were evaluated through the adoption of exploratory factor analysis (EFA) and confirmatory factor analysis (CFA); all the factor loading was satisfactory for the scope of verifying the concept and the quality of the measurement model. The researcher reviewed the drafted questionnaire carefully to ensure that the questions were free from ambiguities, lack of clarity and misunderstanding from the researchers' perspective. Additionally, the questionnaires were given to colleagues in the department to review and certain adjustments were made.

Additionally, to fulfil this purpose, the questionnaire adopted for this study passed through pretesting and piloting before finally being used for the data collection. Questionnaires were developed and administered to 25 staff and 10 customers in five of the selected deposit money banks in Lagos between on the 19th and 23rd December 2016 through the due processes stated in section 4.7 of this chapter. The respondents were the internal control managers, internal auditors and accounting managers in the head offices of the selected banks. In fact, the respondents were selected purposively based on their unique experiences, characteristics, perceptions and possession of the desired information.

4.12 Ethics in Research

Ethical reflections were essential in this research work. Research ethics were guided by the De Montfort University Postgraduate school code of research ethics. Due care was paid to the safety of all the participants involved in providing information. The researcher sincerely paid attention to the major ethical issues of knowledgeable consent, insensitivity, privacy, anonymity and obscurity. A researcher ought to have ambitious standards of professional and personal integrity and truthfulness. It is compulsory to be anxious about the nature of the research location and the safety of all the participants.

Due to the sensitivity of fraud investigation, a letter of introduction (See Appendix 1) was sent to appropriate and relevant authorities of the head offices of the selected Nigerian deposit money banks to assist or enhance the cooperation of the intended respondents; this defined the institutional identity of the researcher and the purpose of the investigation and included a promise of confidentiality and anonymity. In the same vein, the aims and background of the study were clearly stated on the participants' information page included in the questionnaire given to the respondents in order to enhance the participants' understanding.

4.13 Summary

This chapter started with a discussion of the philosophical framework of the methodology and explanation of the research approach employed. Ontological and epistemological (Positivist and interpretivist) approaches were adopted for this study to achieve the target aims and objectives and to build a foundation for generalization of its findings and results. The population and sample of the study, which included the staff of the ten selected deposit money banks in Nigeria, were vividly described. Interviews and a questionnaire consisting of fixed closed structured questions were the main instruments and methods used for the data collected from a considerable number of the Nigerian deposit money bank staff; the procedures were explained in detail. The processes required to collect and analyse data from a primary source and statistical instruments were discussed. Issues of reliability and validity of variable measurement were properly elucidated, as were ethical issues of this research.

CHAPTER FIVE: QUANTITATIVE ANALYSIS

5.0 Introduction

This chapter elucidates the outcomes of the survey analysis that was conducted. The major purpose of conducting the survey was to gather information that would provide a broad and comprehensive view of the characteristics and nature of e-banking frauds in the Nigerian banking institutions. The research survey included two categories of quantitative questionnaires which comprises the administration of 200 for banks' staff and 200 for customers, using different sets of research questions that focused on four aspects: discovery of the e-banking fraud risks that are of high concern in the Nigerian banking sector, the perceived factors that have considerable influence on the increase in e-banking fraud in Nigeria, the current significant mechanisms for e-banking fraud prevention in the Nigerian banking industry and the current significant mechanisms for e-banking fraud detection in the Nigerian banking industry. The questionnaire also included the demographic information of the respondents.

This chapter demonstrates the analysis of the data gathered. The analysis involved two categories. Firstly, presentation of the descriptive measurement, which commenced with the main attributes of the respondents and included the trends of their philosophies and opinions collected from their responses to the questionnaire and analysed by percentages. Secondly, performance of an inferential analysis with use of exploratory factor analysis (EFA) using SPSS for identification of the factors that are significant in each of the hypotheses separately.

In addition, after the constructs had been tested for validity and consistency for the analysis, the model fitness was assessed by confirmatory factor analysis (CFA) through Amos. The responses of customers as e-banking fraud victims, and their attitudes towards prevention and detection of fraud, were used to authenticate certain variables in the hypotheses; these are analysed using chart analysis at the end of this chapter. The outcomes of this chapter are based on statistical processes used to classify and recognize relationships that disprove or prove the hypotheses stated below.

5.1 Examination of Data and Missing Data

A total of 200 questionnaires were distributed to each group: staff respondents and customer respondents. As shown in Table 5.1 below, 169 questionnaires were returned from the staff and 156 from the bank customers, which equates to 84.5% and 78% return rate of questionnaires from the staff and the customers respectively. The data analysis, commenced with the checking of missing data and data entry. It is very important to have some critical insight into data analysis and characteristics (Hair et al., 2010). Therefore, to obtain a high degree of precision, appropriateness, correctness and accuracy in the data entry procedure, a double check was conducted.

The verification of all entry case by case was made in the first entry, while descriptive statistics, which include frequency distribution statistics and the mean, were calculated and verified. The computation of the frequency distribution statistics assisted in discovering two errors in the process of data entry and confirmed the accuracy and correctness of the data entry. In verification the completeness of the returned questionnaires, it was discovered that four staff questionnaires and six customer questionnaires were missing data for constructing measurement sections, with up to at least 25 questions unanswered from each of them.

These questionnaires were completely excluded from the preliminary analysis. In relation to the missing cases, this might be due to reluctant attitudes and lack of understanding of the respondents on how to answer or react to some questions they might have considered sensitive, as is the nature of this study. The correctness and accuracy of the data entered in the data set was approximately 97.63% in the case of the 169 returned staff questionnaires, while approximately 96.15% of the 156 returned customer questionnaires were filled in correctly. And also, the customer questionnaires, 156 and 150 useable samples, respectively were retained for further analysis, which represents 78% staff and 75% customer response rate (see Table 5.1). This is shown that, the respondents really valued the significance of the study in relation with the effects of fraud in the Nigerian banking industry.

Table 5.1: Participating Banks

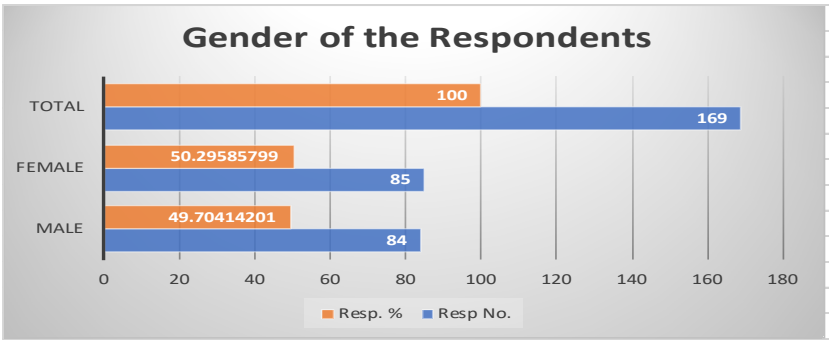
	Staff Questionnaires				Customer Questionr	
	Question.		Returned	Useable	Returned	Useable
BANKS	Distribut.		Qestion.	Question	Question	Question
A	20		20	19	16	16
B	20		20	18	16	15
C	20		13	13	15	15
D	20		16	16	18	14
E	20		12	12	17	17
F	20		16	16	15	15
G	20		18	18	14	14
H	20		18	18	15	14
I	20		18	17	15	15
J	20		18	18	15	15
	200		**169**	**165**	**156**	**150**

Source: Survey Result (2017).

Table 5.1 above indicates that Nigerian bank's staff and customers responded well because of the research phenomenon, which is a current issue in the Nigeria industry and because the appropriate departments were selected. Despite that, securing access to the head offices of Nigerian banks was tremendously tough, the staff and selected customers responded very well.

5.2 Demographic Data of Respondents

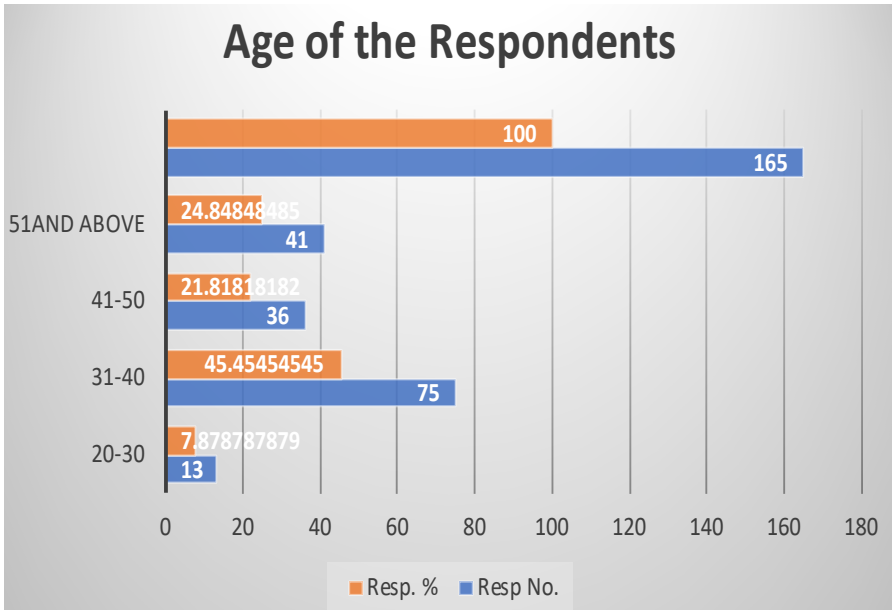
Figure 5.1: Gender of the Respondents



Source: Survey Result (2017)

Figure 5.1 above summarizes demographic participation in the questionnaire survey. Even though more male managers (84; 50.9%) participated in the survey than female managers (81; 49.1%), the disparity between genders is not as noticeable and gender issue has no significant impacts on this phenomenon.

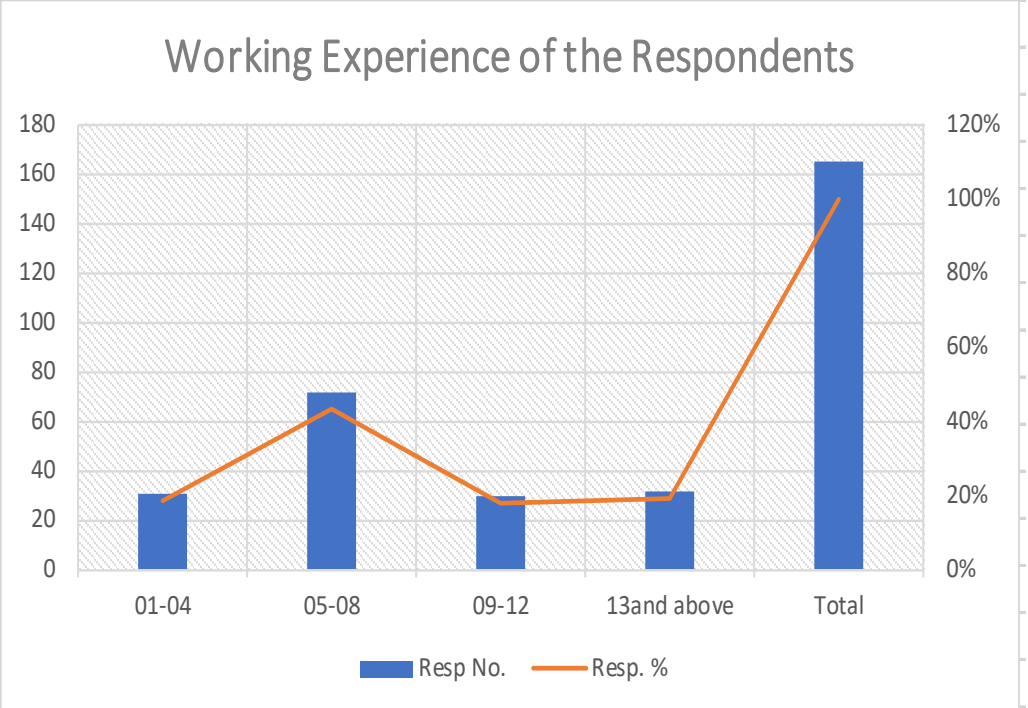
Figure 5.2: Age of the Respondents



Source: Survey Result (2017).

It's obvious in the Figure 5.2 that most of the respondents fall within the age range of 31 years and above, which represented 92% (152) of the total of 165 samples; this is the most active age category in any banking industry. The group aged between 20 and 30 years of 8% (13) can be deduced to have minimal work experience and personal experience related to the phenomenon of e-banking fraud and its prevention and detection compared with the 152 respondents aged 31 years and above. Therefore, the data collected from the mature and experienced participants are valid and authentic.

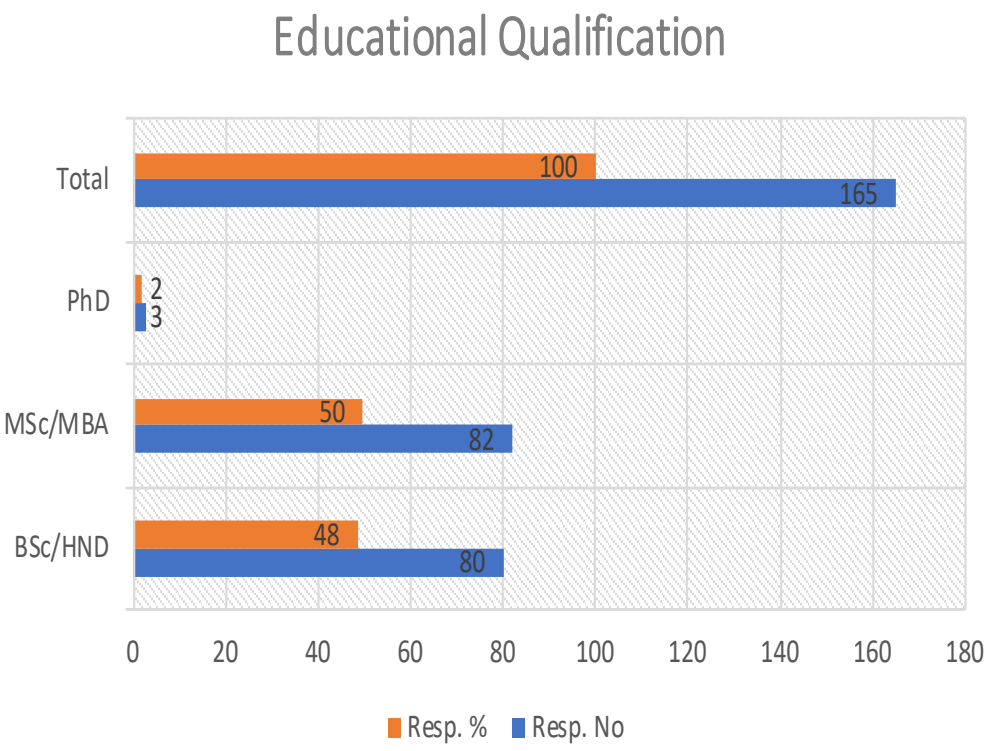
Figure 5.3: Working Experience of the Respondents



Source: Survey Result (2017).

Correspondingly, Figure 5.3 also confirms that most of the participants in the questionnaire survey had been working in the banking industry for at least five years, while the participants that had been working in the banking industry for four years and below were very few. Therefore, most auditors, fraud investigators, bank managers and team leaders in the Nigerian banking industry have been working and have work experience of five years and above. This represents 81.5% of the total samples of 165 that have adequate knowledge and substantial experience of e-banking fraud and its significant impact on financial institutions. This shows that, most of the participants have experienced the incidences of e-banking frauds in their banks and the mechanisms used to prevent and detect it. Therefore, the information collected is valid and authentic.

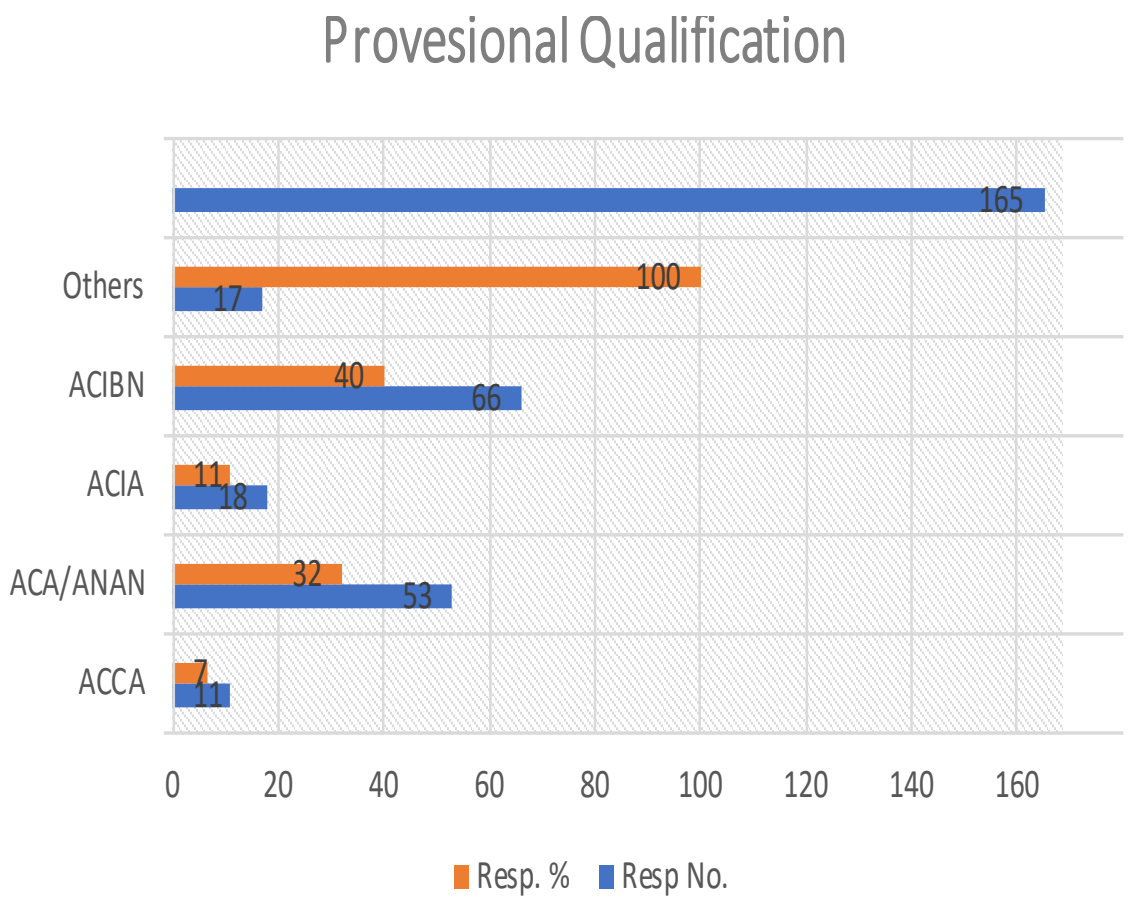
Figure 5.4 Educational Qualification Level



Source: Survey Result (2017).

Figure 5.4, also presents the academic qualifications of the respondents. Out of the 165 participants, 50.6% had acquired a master's degree and 47.6% had bachelor's degrees, while the remaining 1.8% had a doctorate degree. This indicates that all respondents were educated and had knowledge and experience of academic research, its relevance and importance in the academic realm and for the national economy generally, Therefore, the information given would be relevant and reliable to decide on the current phenomenon.

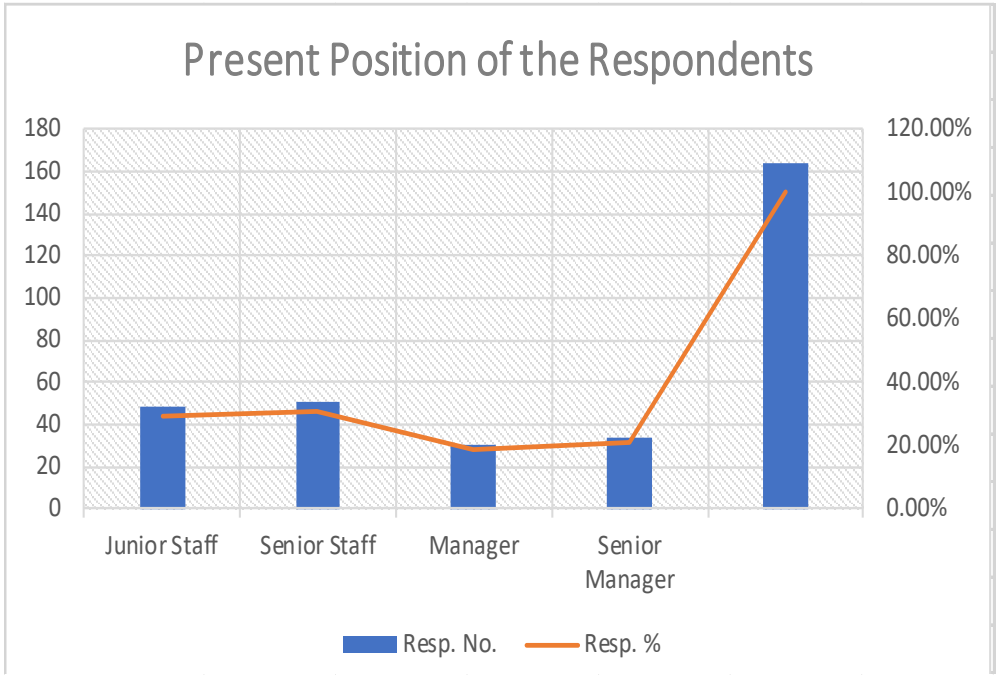
Figure 5.5 Professional qualifications



Source: Survey Result (2017).

In the same vein, Figure 5.5, presents a total of 165 respondents in which 151 respondents (89.9%) were members of professional bodies of bankers, accountants and administrators in addition to their academic qualifications, while 116 of them (69%) were managers. The respondents of the questionnaire survey are therefore the experts in financial industries and possess practical knowledge and different experiences of e-banking fraud prevention and detection. Therefore, the data collected is relevant and reliable.

Figure 5.6 Present Position of the Respondents



Source: Survey Result (2017).

Figure 5.6. A total of 165 respondents from which (70%) were members of senior staff, managers and senior managers were managers. The respondents of the questionnaire survey are therefore experts in financial industries and possess practical knowledge and different experiences of e-banking fraud prevention and detection. Hence, the data collected is relevant and reliable.

5.3 Frequency Analyses of the Responses

The section of analyses provides answers to research questions 1 to 4.

5.3.1 E-banking fraud that are of high concern in Nigeria Banks

Research Question 1: What are the e-banking fraud risks that are of high concern in the Nigerian banking sector?

Table 5.2 E-banking fraud that are of high concern

S/N	E-banking Frauds	SA	A	U	D	SD
B1	Internet Banking Fraud	73.90%	18.20%	1.20%	3.60%	3.00%
B2	Telephone Banking Fraud	66.10%	24.80%	2.40%	4.20%	2.40%
B3	Credit and Debit Card Fraud	63.00%	25.50%	3.00%	4.80%	3.60%
B4	Automated Teller Machine Fra	73.90%	17.60%	3.60%	3.60%	1.20%
B5	E-cheque Fraud	60.00%	24.20%	6.70%	5.50%	3.60%
B6	Mobile Banking Fraud	72.70%	19.40%	1.80%	3.60%	2.40%

Source: Survey Result (2017).

There are various current e-banking fraud risks that are of high concern for the Nigerian banking industry. As shown in Table 5.2, it is obvious that there has been an extensive growth in dependence on technology by Nigerian banking industry. E-banking frauds continue to increase in sophistication, frequency and volume. Therefore, it is not astonishing that the top three areas of e-banking frauds in the Nigerian banking sector that are giving restless nights and challenges to the survey respondents were internet banking frauds, mobile banking and automated teller machine frauds.

This corroborated with the national trend, as reported by the Nigeria Electronic Fraud Forum (NeFF) that ATM, Web and POS were the top three channels used to perpetrate fraud by the fraudsters in 2015. While, in 2016, Mobile, ATM and Web were the most e-banking channels used to perpetrate fraud (NeFF, 2016). Thus, it can be deduced that ATM, Mobile and Internet are the focus e-banking channels for fraud perpetrators in the Nigerian banking institutions.

5.3.2 Contributing Factors to the E-banking Fraud Increase in Nigeria

Research Question 2: What are the perceived factors that have considerable influence on the increase in e-banking fraud in Nigeria?

Table 5.3: Contributing Factors to the E-banking Fraud Increase

S/N	Contributing Factors	SA	A	U	D	SD
C1	Pressure to meet business and personal targets	51.5%	35.2%	5.5%	5.5%	2.4%
C2	Inadequate fraud detection tools	37.0%	45.5%	1.2%	12.1%	4.2%
C3	Collusion between employees and external parties	41.2%	33.9%	3.0%	14.5%	7.3%
C4	Lost cards, stolen personal identification data	52.7%	34.5%	1.8%	7.3%	3.6%
C5	Changes to strategies without changing in business procedures	38.2%	38.2%	3.6%	15.2%	4.8%
C6	New products without adequate control and training in place	50.3%	35.8%	1.2%	9.7%	3.0%
C7	Lack of a fraud risk framework within the organization	35.1%	42.9%	0.6%	17.3%	4.2%
C8	Difficulty integrating data from various sources	48.2%	35.1%	2.4%	10.7%	3.6%
C9	Difficulty investigating crimes across borders	50.3%	40.8%	1.8%	4.8%	2.3%
C10	Irregular electricity power supply in Nigeria	37.6%	27.9%	3.0%	23.6%	7.9%
C11	Lack of forensic accounting professionals	36.4%	34.5%	3.0%	21.8%	4.2%
C12	Downloading, browsing, chatting and spending long time on soc	33.9%	20.6%	4.8%	22.4%	18.2%
C13	Weak litigation support in prosecution process	44.8%	37.1%	2.4%	13.3%	2.4%
C14	Lack of oversight by senior management on deviations from exi	33.9%	20.6%	4.2%	23.6%	17.6%
C15	Issuing of counterfeit credit cards by the employees of the issue	44.2%	36.4%	3.0%	12.7%	3.6%
C16	System with virus, weak software, lack of antivirus, weak passw	43.0%	38.8%	0.0%	13.3%	4.8%
C17	Lack of customer and staff awareness of fraud incidence	37.6%	43.6%	1.8%	13.9%	3.0%
C18	Lack of dedicated technology tools for investigation and insuffic	38.8%	35.8%	3.0%	15.8%	6.7%
C19	Poor coordination with law enforcement	44.8%	35.2%	2.4%	10.9%	6.7%
C20	Lack of effective and efficient internet network facilities	35.8%	35.2%	6.1%	15.8%	7.3%
C21	Absence of quality forensic analysis	49.1%	32.1%	3.0%	11.5%	4.2%
C22	Use of the same password for different accounts	32.7%	43.6%	0.6%	19.4%	3.6%
C23	Lack of rule of law	45.5%	33.9%	4.2%	12.7%	3.6%
C24	Poor system administration and ineffective maintenance	42.5%	43.6%	2.2%	7.3%	4.4%
C25	Lack of forensic accounting professionals and absence of quality	43.8%	37.6%	5.0%	8.1%	5.6%
C26	Lack of dedicated technology tools for investigation	46.1%	33.9%	0.0%	14.0%	6.0%
C27	Insufficient financial resources	35.8%	42.7%	2.0%	10.5%	8.0%
C28	Infectiveness of law enforcement agency	18.5%	33.7%	0.0%	27.8%	20.0%

Source: Survey Result (2017)

Table 5.3 above, presents the analyses of the findings of the outcome of the survey on the factors that contributing to the increase of e-banking fraud in the banking industries. Quite a lot of respondents agreed that there are several reasons and significant challenges for the increase in e-banking fraud incidents for Nigerian banks. The findings and supported studies are discussed below.

Table 5.3, shows that the pressure to meet business and personal targets, inadequate fraud detection and prevention tools within the organisation and collusion between employees and external parties influence the increase in e-banking fraud. This corroborates with Albrech et al. (2010) illustrated pressure with examples that pressure can be in the form of the following: financial losses, living beyond one's means, business distress, competitors' challenge, greediness, credit crises, personal debt, poor credit management, unexpected financial need, frustration at the work, organizational failure, ineffective performance at the place of work, and lack of promotion at place of work. Kassem and Higson (2012) explained that a person becomes a fraudster when they consider themselves as having financial obligations which are known as non-socially authorized and therefore must be satisfied secretly.

The findings in Table 5.3 presents that lost cards and stolen personal identification data, changing of business strategies without changing business procedures, introduction of new products without adequate control and training in place, lack of a fraud risk framework within the organization for customers, difficulty integrating data from various sources influence the increase of e-banking fraud in the Nigerian banking sector. The findings further shows that, difficulty of investigating crimes across borders, lack of forensic accounting professionals, downloading, browsing, chatting and spending a long time on social media, systems with viruses, weak software, lack of antivirus, weak passwords and so on, included weak litigation support in the prosecution process, lack of oversight by senior management of deviations from existing procedure and also, issuing of counterfeit credit cards by the employees of the issuing company enhance fraud perpetration in Nigerian banking institution.

In the same disposition, Salim (2014) online-banking fraud can be initiated from anywhere in the world by involving many perpetrators of various nationalities and use of several servers from different nations. Likewise, the European Central Bank (2014), in its survey of card fraud, reported that card payment fraud is one of the major means of fraud; for example, counterfeit cards, cards not received, lost and stolen cards. The author of this report further elucidated that contemporary mobile devices and their operating systems were not intentionally produced for the security of financial payment: the transmission of personal data and sensitive payment using radio technology exposes mobile payment to risks.

Furthermore, lack of customer and staff awareness of fraud incidence is a great challenge to prevention and detection of e-banking fraud, lack of dedicated technological tools for investigation, insufficient resources and the episodic electrical power supply in Nigeria are challenges to e-banking fraud prevention and detection in Nigerian banking industry. This supported by CIFAS, (2009), the costs of managing e-banking fraud risk and the number of electronic banking fraud incidents are always increasing due to the sophisticated techniques used by electronic banking criminals.

In the same vein, analysis of the findings in Table 5.3 prove that lack of effective and efficient internet network facilities, the absence of quality forensic analysis, using the same password for different accounts, lack of rule of law, that the ineffectiveness of law enforcement agencies contributed, poor system administration and ineffective maintenances, lack of forensic accounting professionals and absence of quality forensic analysis, lack of dedicated technology tools for investigation are the major factors that are contributing to the increase of e-banking fraud in the Nigerian banking institution. Similarly, Deloitte (2015), in the study “India Banking Fraud Survey”, discovered that there is an increase in online fraud occurrence in the banking sector because of the lack of tools and technology to discover the potential red flags.

5.3.3 Mechanisms for E-Banking Fraud Prevention

Research Question 3: What are the current significant mechanisms for e-banking fraud prevention in the Nigerian banking industry?

Table 5.4: Mechanisms for E-Banking Fraud Prevention

S/N	Preventive Mechanisms	SA	A	U	D	SD
D1	Corporate code of conduct	59.40%	34.50%	1.20%	3.60%	1.20%
D2	Carrying out of internal investigation	63.60%	30.90%	0.60%	3.60%	1.20%
D3	Dedicated forensic technology tools for investigat	60.60%	30.90%	3.00%	4.80%	0.60%
D4	Intelligence gathering mechanisms	67.30%	26.10%	1.20%	4.80%	0.60%
D5	Employment of bank verification number (BVN) a	71.50%	23.60%	1.20%	3.00%	0.60%
D6	Use of token card, PINsentry card, passcode, mem	61.20%	31.50%	1.20%	5.50%	0.60%
D7	Collaboration with government, regulators, law e	60.60%	33.90%	0.60%	3.60%	1.20%
D8	American Express SafeKey, MasterCard SecureCod	59.40%	29.10%	1.80%	9.10%	0.60%
D9	Automated Address Verification Service (AVS)	49.70%	36.40%	7.30%	6.10%	0.60%
D10	Checking for cards that are being used fraudulent	54.50%	30.90%	1.80%	8.50%	8.50%
D11	Fraud awareness training	68.50%	29.10%	1.20%	0.60%	0.60%
D12	Employee background check	63.00%	29.10%	3.00%	4.20%	0.60%
D13	Fraud control strategies, regulations, internal con	49.10%	37.00%	0%	10.90%	3.00%
D14	Reporting the incident to a law enforcement ager	21.80%	55.80%	0%	21.20%	1.20%
D15	Asking the individual in question to resign	44.20%	38.80%	3.60%	12.10%	1.20%
D16	Upgradation of technology to combat fraud	44.20%	44.80%	3.60%	6.10%	1.20%
D17	Fraud risk assessment	49.10%	24.80%	1.20%	23.60%	1.20%
D18	Fraud control organization structure	46.10%	37.60%	1.20%	13.90%	1.20%
D19	Clearly defined reporting structure	37.60%	22.40%	3.60%	20.00%	16.40%
D20	Dedicated fraud investigative team from CBN	50.90%	36.40%	0.60%	11.50%	0.60%
D21	Use of personal identification number and autom	37.60%	21.60%	3.60%	21.20%	16.40%
D22	Card Security Code (CSC)	49.20%	36.40%	0.60%	12.70%	0.60%
D23	Third party due diligence	46.70%	43.00%	0%	9.10%	1.20%
D24	Customer screening against negative list	38.20%	47.90%	0%	12.70%	1.20%
D25	Whistle-blower hotline policy	44.20%	25.50%	3.00%	15.20%	12.10%
D26	Data mining	44.20%	42.40%	0.00%	12.70%	0.70%
D27	Corporate governance	48.50%	36.40%	1.20%	9.10%	4.80%

Source: Survey Result (2017)

Several respondents agreed that mechanisms need to be implemented for effective e-banking fraud prevention in the Nigerian banking sector. As shown in Table 5.4, that employment codes of conduct, carrying out of internal investigations, dedicated forensic technology tools for investigation, fraud risk assessment, fraud control organization structure, use of personal identification number and automated phone call with a registered phone number, dedicated fraud investigative team from CBN, card security code (CSC), and employing intelligence gathering mechanisms would have a positive influence on e-banking fraud prevention. This supported by Mac Freddie, (2015) in the study of "Fraud Mitigation Best Practices" fraud risk management policies and procedures are appropriate and significant for fraud prevention, detection, investigation, reporting policies, resolution and communicating them to the relevant stakeholders.

Moreover, analysis of the finding in Table 5.4 shows that, the respondents agreed that employment of a bank verification number (BVN), the use of token card, PINsentry card, passcode, memorable word, personal identification number and automatic phone call with registered phone number; collaboration with government, regulators, law enforcement, academia and other partners Verified by Visa and Mastercard Secure Code, Automated Address Verification Service (AVS) and Card Security Code (CSC), checking for cards that are being used, and introduction of fraud awareness training, would play significant roles in prevention of e-banking fraud. This corroborated by Phua (2010) survey, the authors concluded that, electronic banking fraud prevention focused on fraud prevention software such as Smart Card Authentication, One Time Passwords and Biometric Authentication. Authors further and testify that biometric technology provides a better authentication technique and improves the security.

Furthermore, the analysis in Table 5.4 agreed that, the adoption of employee background checks would enhance fraud prevention, fraud control strategies, regulations and internal control policies; reporting the incident to a law enforcement agency; that upgrading technology to combat fraud, supported third party due diligence, customer screening against negative list, whistle-blower hotline policy, data mining and corporate governance would serve as a significant mechanism for preventing e-banking frauds. Nance and

Straub (1988) and Holling and Clark (1983) supported that information security policies about the organisational policies would prevent potential fraudulent from being committed. These author studies suggested four key areas of policy improvement that are indispensable in preventing fraud. These key areas included the full understanding of fraudsters behaviour, the dissemination of crucial information on organisational policy, the broad casting sanctions, and the implementation and enforcement of sanctions.

5.3.4. Mechanisms for E-Banking Fraud Detection

Reseach Question 4: What are the current significant mechanisms for e-banking fraud detection in the Nigerian banking industry?

Table 5.5: Mechanisms for E-Banking Fraud Detection

S/N	Detection Mechanisms	SA	A	U	D	SD
E1	customers' complaints.	62.50%	29.80%	0.60%	5.40%	1.80%
E2	Auto. data analysis and monitoring software	45.20%	44.00%	0.60%	7.10%	3.00%
E3	Online reconciliation of account enhances e-banking fraud	36.90%	52.40%	3.60%	5.40%	3.60%
E4	Fraud risk assessments and investigations	43.50%	47.00%	0.60%	6.50%	2.40%
E5	Fraud detection and monitoring system	54.80%	38.10%	0.60%	4.80%	1.80%
E6	Use of CCTV at point of transaction	55.40%	25.00%	0.60%	13.10%	6.00%
E7	Monitoring of the internet	53.60%	32.70%	1.20%	8.90%	3.60%
E8	Implementation of banking verification number (BVN) app	73.20%	20.80%	1.20%	3.00%	1.80%
E9	Forensic Computer and accounting approaches.	44.60%	35.70%	2.40%	16.70%	0.60%
E10	Internal whistle-blowers.	52.70%	40.00%	3.60%	7.30%	5.50%
E11	Effective response plan.	51.50%	36.40%	1.20%	9.10%	1.80%
E12	Data mining.	40%	25.50%	3.60%	17%	13.90%
E13	Fraud controls and monitoring teams	53.40%	27.00%	0.50%	12.10%	7.00%
E14	Monitoring the phishing-related websites.	51.60%	34.70%	1.20%	9.90%	2.60%
E15	Anonymous complaints.	73.20%	20.80%	1.20%	3.00%	1.80%
E16	Fraud detective system software.	42.60%	37.70%	2.40%	16.70%	0.60%
E17	Internal surveillance equipment.	50.70%	42.00%	0%	7.30%	0%
E18	ATM monitoring surveillance.	53.50%	34.40%	1.20%	9.10%	1.80%
E19	Internal and external auditors.	43%	22.50%	3.60%	17%	13.90%
E20	Law enforcement agents.	35.40%	30.00%	5.50%	13.10%	16.00%

Source: Survey Result (2017)

Many of respondents agreed that there are numerous mechanisms for e-banking fraud detection in Nigerian banking sector. As shown in Table 5.5, 85percent of the respondents posted that e-banking frauds were detected through customers' complaints, automated data analysis and transaction monitoring software, online reconciliation of accounts, and fraud risk assessments and investigations, fraud detection and monitoring systems, use of CCTV at point of transaction, internal surveillance equipment, ATM monitoring surveillance, through internal and external auditors, use of monitoring of the internet software to detect and close malware and phishing-related websites, included use of banking verification number (BVN) approach.

In addition, Table 5.5, the analysis of the respondents on detection mechanisms, the finding proved that, electronic frauds were detected through application of forensic computer and accounting approaches, internal whistle-blowers/anonymous complaints, use of data mining. This also, supported by Bhasin (2015) that, e-banking can be detected through the application of two-dimensional barcodes, biometrics, cheque image processing, data analytics and data mining, contributed to addressing the problems of fraud detection and prevention.

Likewise, Table 5.5 shows that above two-third of the respondents consented that e-banking frauds were detected through fraud controls, monitoring and analysis teams, monitoring phishing-related websites. This is in the same vein with Bhasin (2015), in an investigation into the "Menace of Frauds in the Indian Banking Industry", found that the innovative detection and prevention technology employed by some banks, including Data Glyphs.

5.4 Factor and Confirmatory Analyses

This section discusses the analyses of research questions 2,3 and 4 with the use of inferential analysis which comprised use of exploratory factor analysis and confirmatory factor analysis.

5.4.1 The Factors Analysis of Factor Contributing to E-banking Fraud

Research Question 2: What are the perceived factors that have considerable influence on the increase of e-banking fraud in Nigeria?

5.4.1.1 Assessment of the suitability of the Constructs of Contributing Factor

Have considered the sample size required for factor analysis as stated in section 4.6. 165 samples were used for this study, which is large enough as suggested that the sample size for factor analysis must, not less than 100 samples, 150 samples are moderate, and 300 samples are large enough (Pallant, 2007; Tabachnick & Fidell, 2007). The coefficient of the correlation matrix is greater than 0.3. which is in line as recommended by Tabachnick & Fidell, (2007) that to determine the strong point of the inter-correlations of the variables, the coefficient of correlation matrix must 0.3 or less. Therefore, the data or constructs are suitable for the factor analysis. Furthermore, to examine the factorability of the constructs or data, two statistical fits were generated which are the Kaiser-Meyer-Olkin (KMO) and Bartlett's of sphericity.

The Kaiser-Meyer-Olkin (KMO) KMO examines the variables' adequacy and factorability with the threshold between 0.7 and 0.9 as strongly acceptable or highly satisfactory (Kaiser, 1974). For this study, the KMO measure is 0.952 (see Table 5.6), which is far above 0.6 the minimum value. Therefore, the variables are strongly satisfactory, adequate and dependable for factor analysis. While, the Bartlett's Test of Sphericity for the study is significant (P<.05) and appropriate for the factor analysis.

Table 5.6: KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.952
Bartlett's Test of Sphericity	Approx. Chi-Square	8061.729
	df	435
	Sig.	0

5.4.1.2 Constructs of the Factors Contributing to the E-banking fraud Increase

The constructs represented by "BA1 to BA30". These are grouped into three groups as following:

Group 1 comprises of: difficulty investigating crimes across borders (BA1); insuring of counterfeit bank cards (BA2); collusion between employees and outsiders (BA3); difficulty integrating information from various sources and lack of effective and efficient internet network facilities (BA4); changing of business strategies without changes in business procedures (BA5); lack of fraud risk assessment framework within the organization (BA6); presence of phishing, identity theft, card skimming, vishing, SMS phishing, viruses, deployment of keystroke loggers and trojans, spyware and adware, website cloning and cyber stalking (BA7); lack of sophisticated antivirus software and weak passwords (BA8); episodic electricity power supply in Nigeria (BA9); lack of fraud prevention and detection techniques and tools (BA10).

Group two involves, ineffective encryption backdoors (BA11); weak litigation support in prosecution process (BA12); poor coordination with law enforcement (BA13); lack of rule of law (BA14); introduction of new products without adequate control and training in place (BA15); customer and staff unawareness of fraud incidence (BA16); use of the same password for different accounts (BA17); incompetence of anti-crime security personnel (BA18); inadequate computer knowledge and experience (BA19); lost cards, stolen personal identification data (BA20). While,

Group three contains, pressure to meet business and personal targets (BA21); spending a long time on social media (BA22); lack of oversight by senior management on deviations from existing procedure (BA23); poor system administration and maintenance (BA24); lack of forensic accounting professionals and absence of quality forensic analysis (BA25); lack of dedicated technology tools for investigation (BA26); insufficient financial resources (BA27); lack of competent internal auditors (BA28); ineffective rule of law (BA29); and lack of efficient internet facilities (BA30) (see Appendix 5).

5.4.1.3 Total Variance Exploratory of the Contributing Factors

Table 5.7 Total Variance Explained (TVE)

Compone	Initial Eigenvalues			Extraction Sums of Squared Loadi			Rotation Sums of Squared Loadin		
	Total	% of Var	Cumulati	Total	% of Varia	Cumulative	Total	% of Varia	Cumulative
1	17.423	58.077	58.077	17.423	58.077	58.077	17.337	57.789	57.789
2	1.774	5.913	63.991	1.774	5.913	63.991	1.583	5.278	63.067
3	1.492	4.972	68.963	1.492	4.972	68.963	1.316	4.386	67.453
4	1.264	4.213	73.176	1.264	4.213	73.176	1.31	4.367	71.82
5	1.115	3.717	76.893	1.115	3.717	76.893	1.273	4.244	76.064
6	1.014	3.38	80.273	1.014	3.38	80.273	1.263	4.209	80.273
7	0.874	2.913	83.185						
8	0.826	2.754	85.939						
9	0.737	2.458	88.397						
10	0.673	2.243	90.64						
11	0.648	2.16	92.8						
12	0.477	1.589	94.388						
13	0.308	1.025	95.414						
14	0.266	0.886	96.299						
15	0.228	0.759	97.058						
16	0.176	0.586	97.644						
17	0.148	0.494	98.137						
18	0.14	0.465	98.603						
19	0.104	0.345	98.948						
20	0.077	0.256	99.204						
21	0.058	0.194	99.398						
22	0.052	0.174	99.572						
23	0.033	0.111	99.683						
24	0.025	0.083	99.766						
25	0.017	0.058	99.824						
26	0.015	0.051	99.875						
27	0.014	0.047	99.922						
28	0.012	0.039	99.961						
29	0.007	0.024	99.985						
30	0.004	0.015	100						

The next step was total variance, shown by the eigenvalue which reflects the number of extracted factors that amount to equal to the number of items which are accounted for by factor analysis. The total variance explained table has been grouped into specific sections: initial eigenvalues, extraction sums of squared loadings and rotation of sums of squared loadings. But for the benefit of analysis and interpretation, the researcher is only

concerned with extraction sums of squared loadings. The total variance explained table is used to determine the number of factors to extract which meet the criterion or have an eigenvalue of 1 or more.

In this case the first six factors recorded eigenvalues greater than 1 (17.423, 1.774, 1.492, 1.264, 1.115 and 1.014; see Total column of initial eigenvalues (see Table 5.7). These six factors explain a total of 80.273% of the variance. However, to determine the number of factors to retain out of the six factors with an eigenvalue greater than 1, the scree pot was also considered.

Figure: 5.7: Scree Plot of the Contributing Factors to E-banking Increase

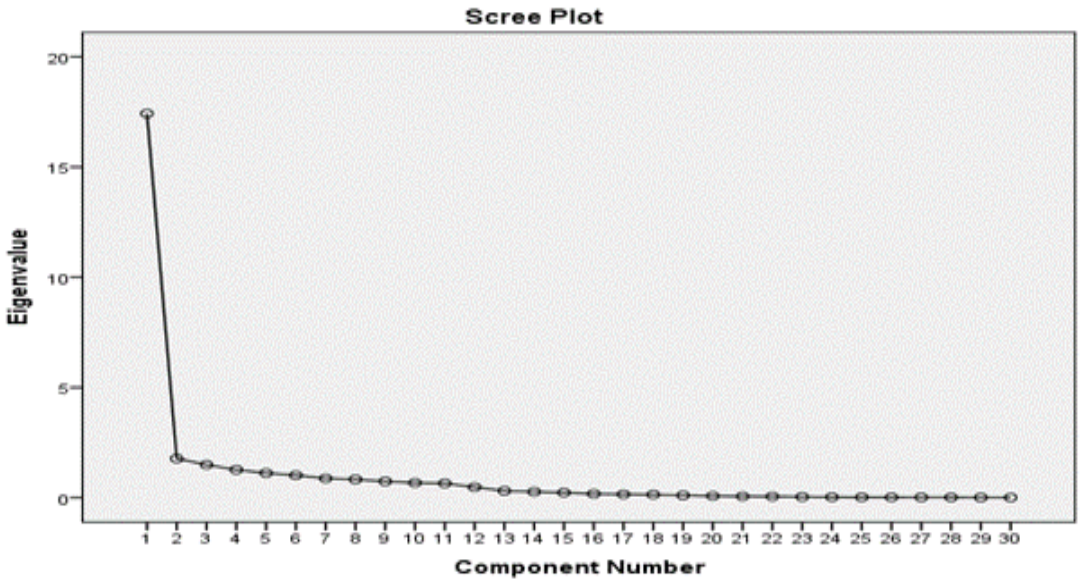


Figure 5.7, presents a scree plot which was used to determine the factors to be retained; this is a line graph of the eigenvalues of all the factors. The main interest is at point where the curve begins to flatten. For instance, in the scree plot of these factors, the curve perfectly flattens between components 23 and 24. Figure 5.7. shows the risen points, which are components or factors 1 to 6 that have eigenvalues higher than 1; these have been retained, while components 7 to 30 that have flattened points and eigenvalues less than 1 were ignored.

Therefore, the results showed that the first six factors were accepted and retained (Table 5.7 & Figure 5.7). These six factors explain a total of 80.273% of the variance, with corresponding extraction sums of squared loadings totalling 80.273%. This simply means the first six retained factors accounted for more than two-thirds of the total variance, which is highly significant. The remaining factors accounted for cumulative of 19.727% (Tables 5.7) which is insignificant.

5.4.1.4 Factor Rotation and Interpretation of Contributing Factors

To obtain the expected outcomes, the researcher ran the Rotated Component Matrix (see Table 5.8) to present the loadings of each of the six components discovered above through eigenvalues. It could be observed from this that most of the cases loaded strongly on the first factor, while the remaining five factors were also well loaded but not as strongly as the first component. The researcher restricted SPSS to select only six factors. Table 5.9, below shows the retained factors or components with their loaded cases or variables which will be worked on with confirmatory factor analysis in the next section. Therefore, the outcome of the factor analysis of the contributing factors to the e-banking fraud increase in Nigerian banking industry can be found in the table5.9 blow with their related variables. The factor analysis has summarised all perceived factors that are contributing to the increase of e-banking fraud in Nigerian into six basic factors which are: operating factors, managerial factors, educational factors, legal factors, technical factors and infrastructural facilities and personnel factors.

Table 5.8 Rotation Component Matrix

Rotated Component Matrix						
	Component					
Factor/Component	1	2	3	4	5	6
Difficulty investigating crimes across borders (BA1)	0.99					
Issuing of counterfeit bank cards (BA2)	0.989					
Collusion between employees and outsiders (BA3)	0.988					
Difficulty integration and ineffective internet network facilities (B	0.984					
Changing of business strategies without changes in business proce	0.981					
Lost cards, stolen personal identification data (BA20)		0.977				
Pressure to meet business and personal targets influence (BA21)		0.974				
Spending long time on social media (BA22)		0.969				
Lack of oversight by senior management on deviations from existing proce		0.963				
Poor system administration and maintenances (BA24)		0.956				
Introduction of new products without adequate control and training in place (BA15)			0.955			
Customers and staff unawareness to the fraud incidence (BA16)			0.943			
Use of the same password for different accounts (BA17)			0.927			
Incompetent of Anti-Crime Security Personnel (BA18)			0.922			
Inadequate computer knowledge and experience (BA19)			0.915			
Weak litigation support in prosecution process (BA12)				0.912		
Poor coordination with law enforcement (BA13)				0.897		
Lack of rule of law (BA14)				0.892		
Ineffective rule of law (BA29)				0.859		
Lack of fraud risk assessment framework within the organization (BA6)				0.637		
Present of phishing, identity theft, card skimming, vishing, SMSishing, viruses, Deployment of ke					0.782	
Lack of sophisticated antivirus software and weak password (BA8)					0.74	
Lack of fraud prevention and detection technological mechanisms (BA10)					0.727	
Ineffective encryption backdoors (BA11)					0.725	
Lack of effective and efficiency internet facilities (BA30)					0.66	
Irregular electricity power supply in Nigeria (BA9)						0.798
Lack of forensic accounting professionals and absence of quality forensic analysis (BA25)						0.746
Lack of dedicated technology tools for investigation (BA26)						0.482
Insufficient Financial resources (BA27)						0.401
Lack of competent internal auditors (BA28)						0.542
Extraction Method: Principal Component Analysis.						
Rotation Method: Varimax with Kaiser Normalization.						
a. Rotation converged in 7 iterations.						

Table 5.9 The Factor Contributing to E-banking Fraud Increase

The Factor Contributing to E-banking Fraud Increase in Nigerian Bank	
Factors	**Observed Variables**
Operational factors	Difficulty investigating crimes across borders
	Issuing of counterfeit bank cards
	Collusion between employees and outsiders
	Difficulty integrating from various sources
	Changing of business strategies without changes in business procedures
Managerial Factors	Lost cards, stolen personal identification data
	Pressure to meet business and personal targets
	Spending a long time on social media
	Lack of oversight by senior management on deviations from existing procedure
	Poor system administration and maintenance
Educational Factors	Introduction of new products without adequate control and training in place
	Customer and staff unawareness of fraud incidence
	Use of the same password for different accounts
	Incompetence of Anti-Crime Security Personnel
	Inadequate computer knowledge and experience
Legal Factors	Weak litigation support in prosecution process
	Poor coordination with law enforcement
	Lack of rule of law
	Ineffective rule of law
	Lack of fraud risk assessment framework within the organization
Technological Facto	Presence of phishing, identity theft, card skimming, vishing, viruses, deployment c
	Lack of sophisticated antivirus software and weak passwords
	Lack of fraud prevention and detection technological mechanisms
	Ineffective encryption backdoors
	Lack of effective and efficient internet facilities
Infrastructural Facili	Episodic electricity power supply in Nigeria
Personnel Factors	Lack of forensic accounting professionals and absence of quality forensic analysis
	Lack of dedicated technology tools for investigation
	Insufficient financial resources
	Lack of competent internal auditors

In addition, the existent relationship of above latent factors and observed variable in the Table 5.9 were tested through the confirmatory factor analysis in the next section.

5.4.1.5 Confirmatory Factor Analysis of the Contributing Factors

This section confirms the outcome of the factor analysis in the Table 5.9 by testing the hypothesis that, there is the existent relationship between the underlying factors (latent variable) and observed variables in the Table.

5.4.1.5.1. Validity and Reliability of the construct of Contributing Factors

Outcomes of research are pronounced as valid once the procedures and techniques followed and statistical tools used are consistent and reliable; and once validity is recognized, reliability is established (Ullman et al., 2004; Mitchell & Jolley, 2004; Saunders et al., 2012; Bryman, 2008). Reliability and validity are mutually nonexclusive, as both go together with lucidity of ability and understanding of constructs to produce the intended output to the research questions (Obalola, 2010). To test for reliability, the Cronbach's Alpha Test was employed in this research. To ascertain the consistency of the respondents' responses given to 30 items in the questionnaire, a reliability test is required. Cronbach's Alpha (α), with coefficient values between 0 and 1, was also employed to determine the interconnectedness of the responses (Saunders et al., 2012; Tavakol & Dennick, 2011).

A total of 165 respondents' responses were considered useable for the 30 items to assess the perceived factors that have considerable influence on the increase in e-banking fraud in Nigeria. Tests of reliability carried out on the constructs gave a Cronbach's Alpha (α) coefficient value of 0.933. This reliability value is greater than the 0.60 minimum threshold of internal consistency (Nunnaly & Bernstein, 1994). This outcome is a signal that the data possess an acceptable reliability and appropriate for confirmatory factor analysis.

5.4.1.5.2. CFA Model of the Contributing Factor

The model in figure 5.8 below is a CFA model for the data collected from the research survey in Nigerian banks on the perceived factors in the increase in e-banking fraud, analysed through SPSS and Amos. The data are the responses of 165 respondents (sample size), with 30 items on the perceived factors that have considerable influence on the increase in e-banking fraud in Nigeria. CFA was used to evaluate the model fit of latent and observed variables of the phenomenon. Before assessing the fit of the structural model, it is essential to use the Amos program to present a measurement model to confirm the 30 observed variables or measured indicators, written to reflect the 6 latent variables from exploratory factor analysis (EFA) above.

Figure 5.8: Initial CFA Model of Contributing Factor

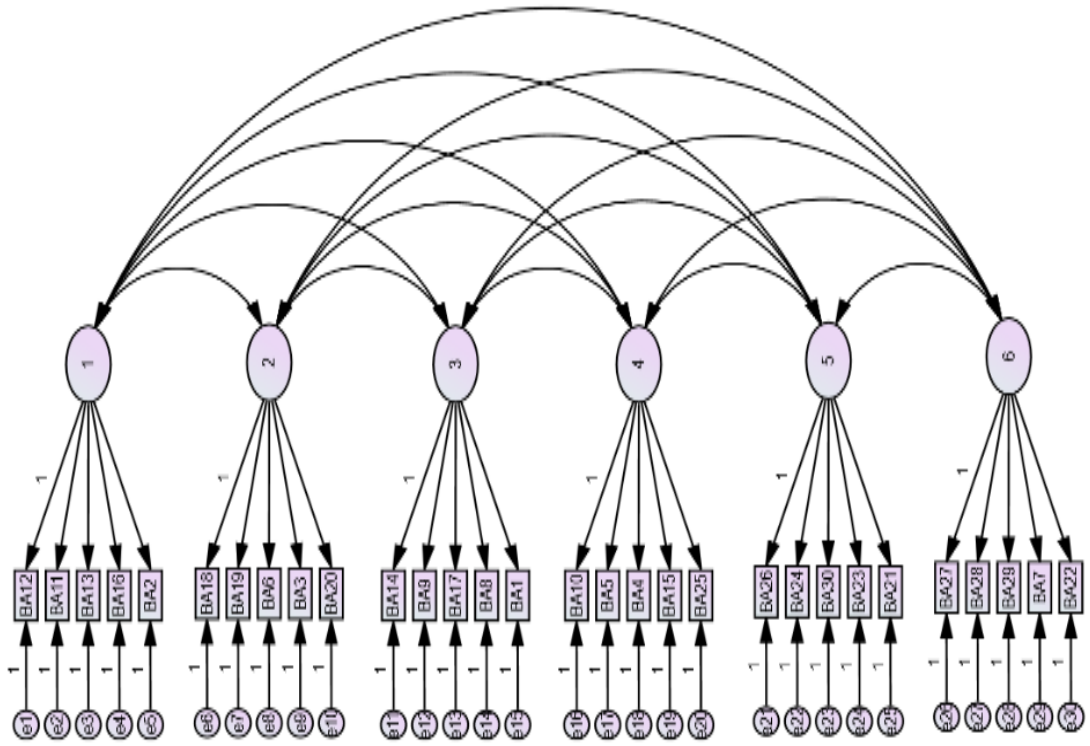


Figure 5.8 above presents the constructed measurement model, which displays loaded factors and estimated items. Items are permitted to load on only one construct without cross-loading and latent variables are permitted to correlate by using SPSS Amos. There are 36 unobserved variables and 30 observed variables in the model (Figure 5.8). The unobserved or exogenous variables are e1, 1, e2, e3, e4, e5, e6, 2, e7, e8, e9, e10, e11, 3, e12, e13, e14, e15, e16, 4, e17, e18, e19, e20, e21, 5, e22, e23, e24, e25, e26, 6, e27, e28, e29 and e30, while the observed or endogenous variables are the following: BA12, BA11, BA13, BA16, BA2, BA18, BA19, BA6, BA3, BA20, BA14, BA9, BA17, BA8, BA1, BA10, BA5, BA4, BA15, BA25, BA26, BA24, BA30, BA23 BA21, BA27, BA28, BA29, BA7 and BA22 (Table 5.8). Therefore, the total number of variables for this model is 66.

Furthermore, each of the 30 measurements or observed indicators has an associated error term or exogenous variable identified as (er). The output model discloses the associated standardized regression weights between the underlying latent factors or variables and observed indicators or variables (see Figure 5.8); characteristically, the 6 hypothesized factors are the factors of e-banking fraud increase, these factors are also known as unobserved or latent variables which determine the correlation among the 30 observed or measured variables. The double-edged arrows among the six factors designate that the researcher presumed that these unobserved variables are correlated and the arrows between the latent factors and the observed variables signify the factors loading or linear regression coefficients. The researcher did not accept that the latent factors totally explained the measured variation in each measured variable.

Table 5.10: Initial Model Fit Measurement of Contributing Factors

CMIN					
Model	**NPAR**	**CMIN**	**DF**	**P**	**MIN/DF**
Default model	75	1116.952	390	0	2.864
Saturated model	465	0	0		
Independence mode	30	8644.711	435	0	19.873
RMR, DFI					
Model	RMR	GFI	AGFI	PGFI	
Default model	0.064	0.697	0.639	0.585	
Saturated model	0	1			
Independence mode	0.436	0.095	0.033	0.089	
Baseline Comparison	NFI	RFI	IFI	TLI	CFI
Model	Delta1	rho1	Delta2	rho2	
Default model	0.871	0.856	0.912	0.901	0.911
Saturated model	1		1		1
Independence mode	0	0	0	0	0
Parsimony-Adjusted Measures					
Model	PRATIO	PNFI	PCFI		
Default model	0.897	0.781	0.817		
Saturated model	0	0	0		
Independence mode	1	0	0		
RMSEA					
Model	RMSEA	LO 90	HI 90	PCLOSE	
Default model	0.107	0.099	0.114	0	
Independence mode	0.339	0.333	0.345	0	

5.4.1.5.3. Interpretation of the Initial Model Fit of Contributing Factors

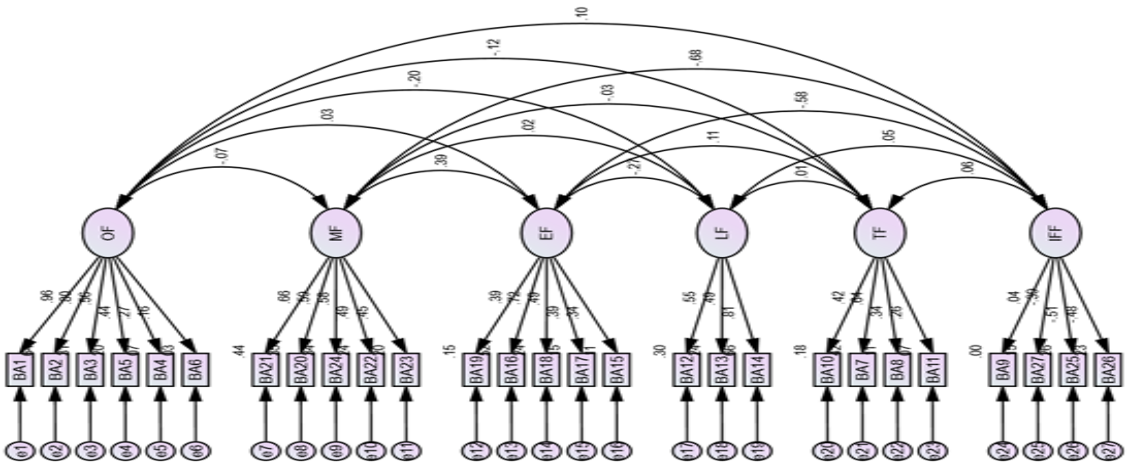
From the results of the model fit estimate in Tables 5.10 it is obvious that the model is not identified or statistically significant. The CMIN/DF is 2.864, which is within the "excellent" threshold between 1 and 3; the CFI is 0.911, which is also within the acceptable range of 0.75–0.95; and SRMR is 0.064, which is within the acceptable range of below 0.08. However, other criteria failed to meet the required threshold. For instance, Chi-Square $X^2 = 1116.952$ at 390 degrees of freedom with $P = 0.000 < 0.05$, which is statically significant: the model does not fit.

Likewise, RMSEA is 0.107, above the 0.06 threshold; PClose is 0.000, less than the 0.05 threshold; and GFI = 0.697, also less than the 0.9 threshold. Therefore, there is need for model modification. As shown in Figure 3.5, a model modification estimate was done through critical examination of regression weights in the modification indices (MI), and three measured variables or parameters that had the highest modification indices or highest discrepancies were completely removed. And the remained 27 observed variables were estimated and re-run to get acceptable fit model or identified model (see the computation below Figure and Table 4.26).

5.4.1.5.4. Modified Model Specification of Contributing Factor

After excluding 3 observed and unobserved variables that had the highest modification indices or highest discrepancies and reallocating 1 measured variable with another fitted latent variable as explained above, there remained 33 unobserved variables (including latent variables) with 27 observed variables for the modified model (Figure 5.9). There are 6 latent variables with 27 structured measured variables in the modified model (simply known as the 6-factor model)

Figure 5.9: Modified Model of Contributing Factor



The six-factor model in Figure 5.9 has parameters of 27 observed or measured variables. The number of variance sample moments in a variance-covariance matrix is 378 which therefor is (p(p+1))/2= ((27(27+1))/2 = 756/2= 378. A saturated model of all paths is 378 + 27 = 405 which means (p(p+3))/2= (27(27+3))/2= 405 (Table 5.11) free parameters that could be assessed. However, in Figure 4.5 above 69 (15 factor covariance, 27 variable error covariance and 27 factor loadings) parameters would be assessed. The degree of freedom for the six-factor model is hence *df* = 378 – 69 = 309. Therefore, the model is identified.

Table 5.11: Modified Model Fit Measurement of Contributing Factors

CMIN					
Model	**NPAR**	**CMIN**	**DF**	**P**	**MIN/DF**
Default model	69	218.492	309	1	0.707
Saturated model	378	0	0		
Independence mode	27	823.783	351	0	2.347
RMR, DFI					
Model	RMR	GFI	AGFI	PGFI	
Default model	0.057	0.915	0.897	0.748	
Saturated model	0	1			
Independence mode	0.134	0.683	0.659	0.635	
Baseline Comparison	NFI	RFI	IFI	TLI	CFI
Model	Delta1	rho1	Delta2	rho2	
Default model	0.735	0.699	1.176	1.217	1
Saturated model	1		1		1
Independence mode	0	0	0	0	0
RMSEA					
Model	RMSEA	LO 90	HI 90	PCLOSE	
Default model	0	0	0	1	
Independence mode	0.091	0.083	0.099	0	

The chi-square goodness-of-fit test value is 216.704 with DF = 309 and p = 1.000 > 0.05 (Table 5.11) which is statistically nonsignificant χ^2 value compared with the degree of freedom *(DF)* indicating that measured variables and estimated variance-covariance data are plausible and fit. Therefore, the six-factor model fits the variance-covariance data

properly. In addition, the researcher considered the maximum likelihood chi-square (ML χ^2) estimation technique.

The Maximum likelihood chi-square ML χ^2 can also be calculated through minimum fit, function value (FMIN) in Table 1 above. The chi-square is χ^2= *(n-1)fm, where "fm"* is the minimum fit function value *and "n"* represents the sample size. The sample size for this model is *165 while FMIN is 1.321 therefore* ML χ^2 = (165 – 1) *1.321* = 216.644(Table 5.11).

In the model measurement Table 5.11, Goodness of Fit Index GFI = 0.916 of the original (observed) covariance matric is suggested by the reproduced (implied) covariance matrix based on one factor model. The GFI is an examination of the degree model fits associated with a single mode (no model) (Schumacker and Lomax ,2004, Blunch, 2012 and Ho, 2006). Goodness of fit (GFI) model fit criterion ranges from 0, signifying poor, to 1, representing excellent fit. Specifically, value greater than or equal to .95 shows an excellent fit (Schumacker and Lomax, 2004 and Blunch, 2012). Thus, in the (Table 5.11), the GFI value of 0.916 indicating of a better fit. It is therefore concluded that the latent factors and observed variables in this present study fits the model properly.

The Adjusted Goodness of Fit Index (AGFI) index is this model analysis is 0.897(Table 5.11). Therefore, Adjusted Goodness of Fit Index is: 1 – [R/df)(1-GFI)] = 1 – [(378/309)(1- 0.916)] = 0.897(Table 5.11). The model fit scale for AGFI is 0 (poor fit) to 1 (excellent fit). Precisely, value adjusted for df with .95 is an excellent mode fit (Schumacker and Lomax, 2004 and Blunch, 2012). Therefore, 0.897 (Table 5.11) is the AGFI model analysis for this study indicating that the model is perfectly fit.

The square root of the mean-squared (SRMR) for this study is 0.056 (Table 5.11) which compliance with the standard scale of "greater than 0.01(poor fit) and lesser than 0.08 (Excellent fit)". Therefore, this indicates that the square root of the inconsistency between the model sample covariance matrix and covariance matrix are very close.

The root means square error of approximation (RMSEA) standard scale rage from 0 to 1. A range of .05 or less is signifying satisfactory model fit while, range of zero is perfectly

fit (Schumacker and Lomax ,2004 and Blunch, 2012). In the current study, the RMSEA value for the hypothesized model is 0.000 (Table 5,11) Therefore, the model is satisfactorily acceptable.

The tucker Lewis index (TLI) range from 0 (poor) to 1 (excellent fit). Typically, value greater than or equal to 0.95 reflects a excellent model fit. The value of TLI for this current study was calculated as [X^2null/*df*null) – (X^2model/*df*model)]/[(X^2null/*df*null) – 1] = [(826.456/351) – (216.704/309)] /[(826.456/351) – 1] = 1.221(Table 5.11). Therefore, the model for this analysis is fit and satisfactory.

The Normed Fit Index (NFI) was calculated as (826.456 – 216.704)/826.456 = 0.7378 (Table 5.11). While Comparative fit index (CFI) for this analysis is 1.000, Incremental Fit Index (IFI) and Relative Fit Index (RFI) are 1.178 and 0.702 respectively (Table 5.11).

The Relative Fit Index (RFI)= [1-[(X^2model/*df*model)/(X^2null/*df*null)] =[1-(216.704/309)/(826.456/351)] = 0.702 (5.11) while the incremental fit index (IFI) = 1 – [(X^2null – X^2model)/X^2null – *df*model)] = [(826.456 – 5216.704)/(826.456-309)] = 1.178 (Table 5.11). Therefore, the hypothesized model for this current analysis is perfectly fit because NFI, CFI, RFI and IFI values are greater than 0.7 threshold. Schumacker and Lomax (2004) and Blunch, (2012) posted that value greater than 0.7 reflects excellent model fit. (Note: X^2model= The default model, model of the discrepancy; *df*model= The default model, model of degrees of freedom; X^2null= The independence model, model of discrepancy; *df*null= The independence model, model of degrees of freedom).

In conclusion, there is correlation between the observed variables and the latent factors which means, operational, managerial problem, educational, technological and infrastructural factors have considerable influence on the increase of e-banking frauds in Nigeria.

5.4.1.5 Discussion of the Findings

This section discusses the outcome of findings from the analyses of the quantitative survey on the perceived factors contributing to the increase of E-banking fraud in Nigerian banking sector. E-banking fraud tends to be perpetrated not only due to the three main factors of the fraud triangle (rationalization, opportunity and financial pressure) but also, as it has been seen from the survey outcomes above, the findings of this in the above section have suggested other seven factors: operational factors, managerial factors, educational factors, technological factors, legal factors, infrastructural factors and personnel factors.

5.4.1.5.1 Operational factors

Operational factors are the factors that emerged through the mode of business operations and attitudes of staff towards the business. These reflected the following issues contribute to the increase of e-banking fraud in the Nigerian banking industry: difficulty investigating crimes across borders, insuring of counterfeit bank cards, collusion between employees and outsiders, difficulty integrating from various sources and lack of effective and efficient internet network facilities, changing of business strategies without changes in business procedures, and lack of fraud risk assessment frameworks within the organization. This matches with Kinkela and Harris (2014), found that frauds involve the teaming up of bank staff with security agents in both national and international networking.

5.4.1.5.2 Technological factors

Technological factors are the factors used or exploited by the perpetrators to hijack or perpetrate frauds on electronic systems, for example phishing, identity theft, card skimming, vishing, SMS phishing, viruses, deployment of keystroke loggers and Trojans, spyware and adware, website cloning and cyber stalking, lack of sophisticated antivirus software and weak passwords, episodic electricity power supply, lack of preventive and detection techniques and tools, and ineffective encryption backdoors.

This agrees with Peotta et al. (2011), who adopted an attack tree model to represent the major attacks on e-banking and how they associate with each other, for example phishing attacks, social engineering, malware to gain control of system devices, and malware and fake web pages for credential theft from an authentic user. Omariba, Moses and Wanyembi (2012) also classified a range of factors contributing to electronic banking fraud, such as port scanners, social engineering attacks, phishing, Trojans, pharming, denial of service, PIN hacking, super user exploits and server bugs.

5.4.1.5.3 Legal and Law Enforcement

Lack of proper legal and law enforcement processes also contribute to the increase of e-banking fraud. These factors include weak litigation support in the prosecution process, poor coordination with law enforcement and lack of rule of law. In addition, corruption in the law enforcement agencies such as courts and police in Nigeria contributes to inadequate prosecutions of fraudsters and investigation of frauds, which has impaired reliability and discouraged some banks from prosecuting those that perpetrate fraud because of fear of an unsuccessful outcome. Prosecution of suspected fraudsters is particularly difficult in a country where the regulators, police, lawyers and judges are vulnerable to bribes (Cule & Fulton, 2009).

5.4.1.5.4 Educational factors

Educational factors could also contribute the upsurge in e-banking fraud; for example, the introduction of new products without adequate control and training in place, customer and staff unawareness of fraud incidence, use of the same password for different accounts, incompetence of anti-crime security personnel, and inadequate computer knowledge and experience. In conjunction with the above, an investigation by Choplin and Stark (2013) found that banking customers are vulnerable to e-banking fraud because of lack of education and awareness.

5.4.1.5.5 Maintenance and Management Factors

Improper maintenance and management contributes to the increase of e-banking fraud which emanated from negative habits of customers towards their bank account facilities, such as loss of bank cards, theft of personal identification data and spending a long time on social media. So also, ineffective performance of management, which could lead to pressure to meet business and personal targets, lack of oversight by senior management on deviations from existing procedure, and poor system administration and maintenance culture give room to perpetration of e-banking fraud in the banking system.

5.4.1.5.6 Personnel Factors

The findings of this study confirm that lack of enough professional skills in the banking business contributes to the increase in e-banking fraud. This includes unavailability of forensic accounting professionals and independent forensic auditors, lack of competent internal auditors, absence of quality forensic analysis, lack of fraud investigation experts, absent of litigation experts and ineffective law enforcement agencies.

5.4.1.5.7 Infrastructural Factors

The findings research revealed that lack of facilities and inadequacy of resources – for example, episodic electricity power supply, lack of dedicated technological tools for investigation, lack of effective internet facilities and insufficient financial resources contribute to the increase of e-banking fraud. This corroborates with the opinion of Deloitte (2015), in the study "India Banking Fraud Survey", which discovered that there is an increase in online fraud occurrence in the banking sector because of the lack of the tools and technology to discover potential red flags.

5.4.2 Factor Analysis of the Prevention Mechanism

Research Question 3. What are the current significant mechanisms for e-banking fraud prevention in the Nigerian banking industry?

5.4.2.1 Assessment of the suitability of the Constructs of Prevention Mechanism

Having considered the sample size required for factor analysis as stated in section 4.6. 165 samples were used for this study, which is large enough as suggested that the sample size for factor analysis must, not less than 100 samples, 150 samples are moderate, and 300 samples are large enough. (Pallant 2005; Tabachnick & Fidell, 2007). The coefficient of the correlation matrix is greater than 0.3. which is in line as recommended by Tabachnick & Fidell, (2007) that to determine the strong point of the inter-correlations of the variables, the coefficient of correlation matrix must 0.3 or less. Therefore, the data or constructs are suitable for the factor analysis. Furthermore, to examine the factorability of the constructs or data, two statistical fits were generated which are the Kaiser-Meyer-Olkin (KMO) and Bartlett's of sphericity.

Table 5.12: KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.775
Bartlett's Test of Sphericity	Approx. Chi-Square	1471.593
	df	171
	Sig.	0

The Kaiser-Meyer-Olkin (KMO) KMO examines the variables' adequacy and factorability with the threshold between 0.7 and 0.9 as strongly acceptable or highly satisfactory (Schumacker & Lomax, 2004). For this study, the KMO measure is 0.775 (see Table 5.12), which is far above 0.6 the minimum value. Therefore, the variables are strongly satisfactory, adequate and dependable for factor analysis. While, the Bartlett's Test of Sphericity for the study is significant (P<.05) and appropriate for the factor analysis (see Table 5.12). Therefore, the constructs for the examination of prevention mechanisms of e-banking fraud in this study are appropriate and satisfied.

5.4.2.2 Total Variance Exploratory of the Prevention Mechanisms

the communalities were examined to ascertain how much of the variance in the variables was accounted for by the extracted factors. Appendix 6 shows that over 100% of the variance in the variables was accounted for the by extraction of the latent variables. This

was achieved after removing all the variables that had extraction values less than 0.3. Thereafter, the eigenvalue reflects the number of extracted factors which amount to equal to the number of items that are accounted to factor analysis.

Table 5.13: Total Variance Explained

Total Variance Explained										
Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings			
	Total	% of Varianc	Cumulative	Total	% of Varianc	Cumulative	Total	% of Varianc	Cumulative %	
1	4.313	22.699	22.699	4.313	22.699	22.699	3.757	19.774	19.774	
2	3.137	16.51	39.209	3.137	16.51	39.209	3.123	16.439	36.213	
3	2.628	13.831	53.041	2.628	13.831	53.041	3.023	15.912	52.126	
4	1.327	6.983	60.024	1.327	6.983	60.024	1.501	7.898	60.024	
5	1.067	5.613	65.637							
6	0.934	4.918	70.555							
7	0.838	4.412	74.967							
8	0.76	3.999	78.965							
9	0.677	3.566	82.531							
10	0.572	3.012	85.543							
11	0.513	2.699	88.242							
12	0.438	2.308	90.55							
13	0.393	2.069	92.619							
14	0.371	1.955	94.574							
15	0.353	1.857	96.431							
16	0.255	1.342	97.773							
17	0.203	1.069	98.843							
18	0.114	0.6	99.443							
19	0.106	0.557	100							
Extraction Method: Principal Component Analysis.										

The eigenvalue table has been grouped into specific sections: initial eigenvalues, extraction sums of squared loadings and rotation of sums of squared loadings. But for the benefit of analysis and interpretation, the researcher was only concerned with extraction sums of squared loadings. The total variance explained table was used to determine the number of factors to extract which met the criterion or had an eigenvalue of 1 or more. These were the first five factors, which recorded eigenvalues greater than 1 (4.313, 3.137, 2.628, 1.327 and 1.067; see Total column of initial eigenvalues in Table 5.13). These six factors explain a total of 65.637% of the variance. However, to determine the number of factors to retain out of the six factors with eigenvalues greater than 1, a parallel analysis was adopted (see Appendix 7).

Systematically, the first eigenvalue obtained from principal component analysis (PCA) in SPSS was compared with the equivalent first result from the random values obtained from parallel analysis. The factor was retained if the eigenvalue from PCA was greater than the criterion result from parallel analysis; if it was otherwise, the factor was rejected. The results show that the first four factors, with eigenvalues of 4.313, 3.137, 2.628 and 1.327, were accepted and retained (see Table 5.13 and Appendix 7). These four factors explain a total of 60.024% of the variance, with corresponding extraction sums of squared loadings totalling 60.024%. This means that the first four retained factors accounted for more than three-fifths of the total variance, which is highly significant. The remaining factors accounted for a cumulative value of 39.97% (see Table 5.13), which is insignificant.

Table 5.14: Rotated Component Matrix

Rotated Component Matrixa				
	Component			
	1	2	3	4
GA1	0.918			
GA2	0.897			
GA3	0.832			
GA4	0.774			
GA5	0.734			
GA6	0.777			
GA7	0.732			
GA8		0.677		
GA9		0.651		
GA10		0.596		
GA11			0.58	
GA12			0.562	
GA13			0.933	
GA14			0.901	
GA15			0.842	
GA16			0.593	
GA17				0.694
GA18				0.632
GA19				0.621
Extraction Method: Principal Component Analysis.				
Rotation Method: Varimax with Kaiser Normalization.				
a. Rotation converged in 4 iterations.				

Moreover, a rotated component matrix in Table 5.14 was used to present the loadings of each of the cases in four components. It could be observed that most of the cases loaded

strongly on the first and third factors, while the second and fourth factors were also well loaded but not as much so as the first and third components; the researcher used SPSS to select only four factors. This corroborates the earlier conclusion and recommendation from the Monte Carlo PCA for parallel analysis, to extract and retain only the first four factors out of the five factors that had eigenvalues greater than 1 (see Table 5.13).

Therefore, the outcomes of the rotated component matrix (RCM) of the loading variables for each of the four selected factors or mechanisms of prevention (Scientific Mechanisms, Awareness and Education Mechanisms, Internal Control and Know Your Customer Mechanisms, and Legal and Synergies Mechanisms are listed below in Table 5.15 with their symbols and latent names.

Table 5.15: Current Preventive Mechanisms for E-banking Fraud

S/N	Components/Factors	Loaded Variables	Symbols
	(Unmeasured Variables)	(Measured Variables)	
1	Scientific Mechanisms	Bank verification number	GA1
		Dedicated forensic technological tools for investigation	GA2
		Use of security code, token cards, MasterCard SecureCode and smart card authentication	GA3
		Use of one-time password, multi-layer passwords and memorable words	GA4
		Use of PII, registered phone number, biometrics and data encryption	GA5
		Availability of closed circuit television (CCTV) security system	GA6
2	Awareness and Education Mechanisms	Timely access to information	GA9
		Consumer education and accounting information protection	GA7
		Effective fraud awareness training and Seminars	GA8
3	Internal Control and	Customer screening and employee background check	GA10
	Know Your Customer Mechanisms	Automated address verification service (AVS) and automated phone call	GA14
		Fraud internal control structure	GA13
		Intelligence gathering mechanisms	GA12
		Clearly defined reporting structure and effective governance, risk and compliance programmes	GA15
		Fraud risk assessment	GA11
4	Legal and Synergies Mechanisms	Effective fraud control policy, regulation and corporate code of conduct	GA16
		Availability of effective whistle-blower hotline policy	GA18
		Collaboration with government, regulator, law enforcement agency and academia	GA17
		Partnership with Foreign Banks.	GA19

Furthermore, the relationship between the latent factors and observed variables in the Table 5.15 were tested and verified through the use of confirmatory factor analysis in the next section.

5.4.2.3 Confirmatory Factor Analysis of the Detection Mechanisms

This section verifies the result of the factor analysis in the Table 5.15 by testing and confirming the hypothesis that, there is the existent relationship between the underlying factors (latent variable) and observed variables in the Table.

5.4.2.3.1 Reliability and Validity of the Prevention Mechanism Constructs

Reliability and validity are mutually nonexclusive, as both go together with lucidity of ability and understanding of prevention mechanism constructs to produce the intended output to the research questions (Obalola, 2010). To test for reliability, Cronbach's Alpha Test of reliability was employed in this research. To ascertain the consistency of the respondents' responses given to 19 items produced by EFA, a reliability test was required. Cronbach's Alpha (α) with coefficient values between 0 to 1 was also employed to determine the interconnectedness of the responses (Saunders et al., 2012; Tavakol & Dennick, 2011).

A total of 165 respondents' responses were considered useable for the 19 items to assess the significant impacts of preventive mechanisms on e-banking fraud. Tests of reliability carried out on the constructs gave a Cronbach's Alpha (α) coefficient value of 0.872. This reliability value is greater than the 0.60 minimum threshold of internal consistency (Nunnaly & Bernstein, 1994). The means, the constructs used for the preventive mechanisms of e-banking fraud are valid and reliable for the confirmatory factor analysis.

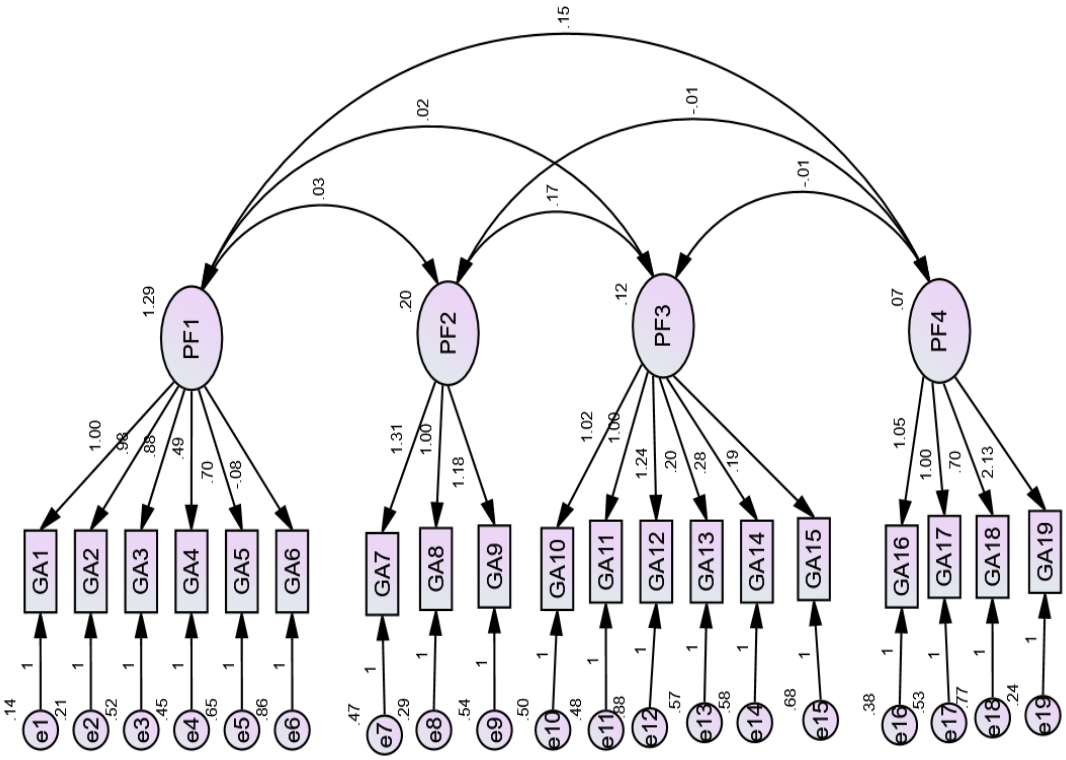
5.4.2.3.2 CFA Model of the Prevention Mechanisms of E-banking Fraud

CFA was used to evaluate the current prevention mechanisms that have a significant impact on e-banking fraud prevention in Nigerian banks. Before assessing the fit of the structural model, it is essential to present a measurement model to confirm the 19 observed variables written to reflect the 4 latent variables in the Table 5.15 above. Figure 5.10 below presents the constructed measurement model which displays loaded factors and estimated items. Items are permitted to load on only one construct without cross-loading and latent variables are permitted to correlate by using Amos in SPSS. There are 4 latent factors (four-factor model): Scientific Mechanisms (PF1), Awareness and Education Mechanisms (PF2), Internal Control and Know Your Customer Mechanisms (PF3), Legal and Synergies Mechanisms (PF4) with their related observed variables which already stated in the Table 5.15 (see Figure 5.10)

Additionally, the four-factor model precisely hypothesized current mechanisms for e-banking fraud prevention in Nigerian banks. These factors are also known as unobserved or latent variables which determine the correlation among the 19 observed or measured variables. The double-edged arrows among the four factors designate that the researcher presumed that these unobserved variables are correlated and the arrows between the latent factors and the observed variables signify factor loadings or linear regression coefficients.

The Figure 5.10, represents the observed or endogenous variables are GA1, GA2, GA3, GA5, GA4, GA6, GA7, GA8, GA9, GA10, GA11, GA12, GA13, GA14, GA15, GA16, GA17, GA18 and GA19, while the unobserved or exogenous variables are e1, PF1, e2, e3, e4, e5, e6, e7, PF2, e8, e9, e10, PF3, e11, e12, e13, e14, e15, e16, PF4, e17, e18 and e19. In addition, each of these 19 measurement indicators variables has a related error term identified as (er); the output model unveils the associated standardized regression weights between the underlying latent factors and observed variables (See Figure 5.10).

Figure 5.10 Confirmatory Model of Prevention Mechanisms



Also, the standard illustration in the program Amos makes it clear that the errors are also unobserved factors. Therefore, the total number of variables in the model (Figure 5.10) is 42, which is composed of 19 observed or endogenous variables and 23 unobserved or exogeneous variables.

5.4.2.3.3 Interpretation of the Model Fit Analysis of Prevention Mechanisms

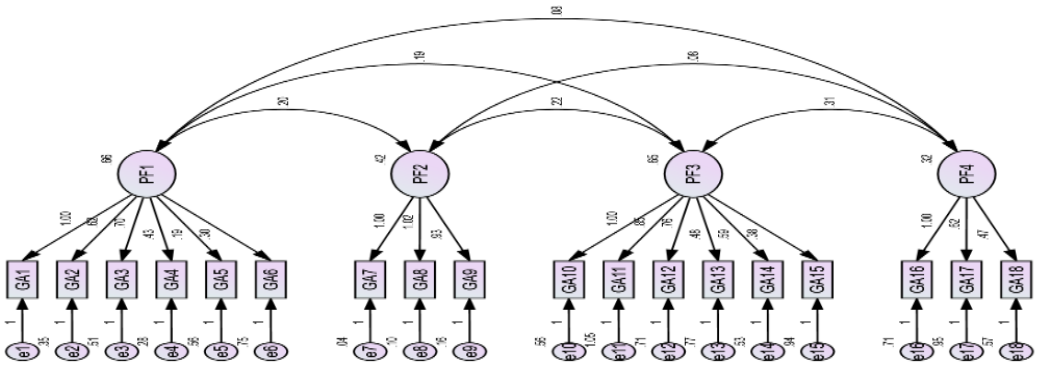
It is obvious from Table 5.16, that the model does not fit because chi-square (X^2) 252.060, P = 0.000 (< 0.05). Despite that, all other criteria – CMIN/DF, RMR, GFI, AGFI, NFI, RFI, IFI, TLI, CFI, RMSEA and PCLOSE – are within the acceptable threshold but not within the excellent threshold. Therefore, there is a need for model modification, which is presented in the next section.

Table 5.16 Model Fit Analysis of the Prevention Mechanisms (PM)

CMIN					
Model	**NPAR**	**CMIN**	**DF**	**P**	**CMIN/DF**
Default model	44	252.06	146	0	1.726
Saturated model	190	0	0		
Independence mode	19	1538.839	171	0	8.999
RMR, DFI					
Model	RMR	GFI	AGFI	PGFI	
Default model	0.059	0.087	0.83	0.668	
Saturated model	0	1			
Independence mode	0.247	0.45	0.389	0.405	
Baseline Comparison	NFI	RFI	IFI	TLI	CFI
Model	Delta1	rho1	Delta2	rho2	
Default model	0.836	0.808	0.924	0.909	0.922
Saturated model	1		1		1
Independence mode	0	0	0	0	0
RMSEA					
Model	RMSEA	LO 90	HI 90	PCLOSE	
Default model	0.067	0.052	0.08	0.028	
Independence mode	0.221	0.211	0.231	0	

5.4.2.3.4 **Modified Model Fit Measurement of Prevention Mechanisms (PM)**

The four-factor model in Figure 5.11 has parameters of 18 observed or measured variables. The researcher revisited the modification indices and removed only one measured variable, GA19, which had the highest modification indices of 28.737 in the regression. This was because, if the researcher repeated the analysis treating the



regression weight for using GA19 to predict GA16 as a free parameter, the discrepancy would fall by at least 28.737. Therefore, it is justified to remove G19 and re-run the model (see Figure 5.10) which its outcome could be found in the Figure 5.11.

Figure 5.11: Modified Model of Fit of Prevention Mechanisms

Table 5.17 Model Fit Analysis of the Prevention Mechanisms

CMIN					
Model	NPAR	CMIN	DF	P	MIN/DF
Default model	42	80.946	129	1	0.627
Saturated model	171	0	0		
Independence mode	18	837.531	153	0	5.474
RMR, DFI					
Model	RMR	GFI	AGFI	PGFI	
Default model	0.039	0.948	0.931	0.715	
Saturated model	0	1			
Independence mode	0.162	0.561	0.509	0.502	
Baseline Comparison	NFI	RFI	IFI	TLI	CFI
Model	Delta1	rho1	Delta2	rho2	
Default model	0.903	0.885	1.068	1.083	1
Saturated model	1		1		1
Independence mode	0	0	0	0	0
RMSEA					
Model	RMSEA	LO 90	HI 90	PCLOSE	
Default model	0	0	0	1	
Independence mode	0.165	0.154	0.176	0	

5.4.2.3.5 Interpretation of the Modified Model Fit of PM

The number of variance sample moments in variance-covariance matrix is 171 which therefor is (p(p+1))/2= ((18(18+1))/2 = 342/2= 171. A saturated model of all paths is 171 + 18 = 189 which means (p(p+3))/2= (18(18+3))/2= 189 (Table 5.18) free parameters that could be estimated. However, in Figure 5.11 above 42 (6 factor covariance, 18 variable error covariance and 18 factor loadings) parameters would be assessed. The degree of freedom for the four-factor model is hence *df* = 171 – 42 = 129189 (Table 5.17). Therefore, the model is identified.

The Chi-square goodness-of-fit test value is 80.946 with df = 129 and p < 1.000 189 (Table 5.17) which is statistically nonsignificant χ^2 value comparative with the degree of freedom *(df)* indicating that measured variables and estimated variance-covariance data

are plausible and fit. Therefore, the four-factor model fits the variance-covariance data properly. In addition, the researcher considered the maximum likelihood chi-square (ML χ^2) estimation technique.

Furthermore, the Maximum Likelihood Chi-square ML χ^2 can also be calculated through minimum fit function value (FMIN) in 189 (Table 5.17) above. The chi-square is $\chi^2 = (n-1)fm$, *where "fm"* is the minimum fit function value *and "n"* represents the sample size. The sample size for this model is *165 while FMIN is 0.494 therefore* ML χ^2 = (165 – 1) *0.494* = 81

In the model Figure 5.11, Goodness of Fit (GFI) = 0.948 of the original (observed) covariance matric is suggested by the reproduced (implied) covariance matrix based on one factor model. Goodness of fit (GFI) model fit criterion ranges from 0, signifying poor, to 1, representing excellent fit. Specifically, value greater than or equal to .95 shows an excellent fit (Schumacker and Lomax ,2004). Thus, in the 189 (Table 5.17), the GFI value of 0.948 indicating of a better fit. It is therefore concluded that the latent factors and observed variables in this present study fits the model properly.

The Adjusted Goodness of Fit (GFI) index of this model analysis is 0.931(Table 5.17). Therefore, AGFI index is: 1 – [R/df)(1-GFI)] = 1 – [(171/129)(1- 0.948)] = 0.931. The model fit standard scale of Adjusted Goodness of Fit ranges from 0 (poor fit) to 1 (excellent fit). Precisely, value adjusted for degree of freedom with .95 is a satisfactory mode fit (Blunch, 2012). Therefore, 0.931 189 (Table 5.17) is the AGFI model analysis for this study. The indicates that the model is perfectly fit.

The square root of the mean-squared (SRMR) for this study is 0.039189 (Table 5.17) indicating that the square root of the inconsistency between the model sample covariance matrix and covariance matrix is very close.

The RMSEA scales from 0 to 1, with lesser values representing better model fit. A range of .05 or less is signifying satisfactory model fit while, range of zero is perfectly fit (Byrne, 2016). In the current study, the RMSEA value for the hypothesized model is 0.000 189 (Table 5.17). Therefore, the model is satisfactorily acceptable and perfectly fit.

Tucker-Lewis Index (TLI) is used to equate projected or alternative model with a null model. The TLI range from 0 (poor fit) to 1 (excellent fit). Typically, value greater than or equal to 0.95 reflects an excellent model fit. The value of TLI for this current study was calculated as $[X^2null/dfnull) - (X^2model/dfmodel)]/[(X^2null/dfnull) - 1] = [(837.531/153) - (80.946/129)] /[(837.531/153) - 1] = 1.083\ 189$ (Table 5.17). Therefore, the model for this analysis is satisfactory fit.

The Normed Fit Index (NFI) was calculated as $(837.531 - 80.946)/837.531 = 0.903\ 189$ and Comparative Fit Index (CFI) is 1.000 189 (Table 5.17) while Incremental Fit index (IFI) and Relative Fit Index (RFI) are 0.885 and 0.702 respectively.

Therefore, the hypothesized model for this current analysis is perfectly fit because NFI, CFI, RFI and IFI values are greater than 0.7.

Inconclusion, there is correlation between the observed variables and the latent factors of the hypothetical model which means, scientific mechanisms, awareness and education mechanisms, internal control, know your customer (KYC) mechanisms, legal and synergies mechanisms are current anti-fraud mechanisms of the e-banking frauds prevention in Nigerian banking industries. The considerable variables for these hypothesized mechanisms of e-banking prevention were discussed and summarized below.

5.4.2.4 Discussion of the Findings

The responses of survey questionnaire respondents highlighted four groups of preventive mechanisms of e-banking fraud in Nigeria. According to the survey respondents, the current mechanisms that have been applied by individual banks were grouped as follows: scientific mechanisms, awareness and educational mechanisms, internal control mechanisms, and legal and synergies mechanisms.

5.4.2.4.1 Scientific mechanisms

Scientific Mechanisms are the technological strategies and tools applied to prevent and control e-banking and cyber fraud in the banking industry. Scientific mechanisms are

among of the best ways to prevent e-banking fraud. The quantitative respondents reported that e-banking fraud has been drastically reduced through the introduction of the bank verification number. This is supported by the Central Bank of Nigeria, which through the Bankers' Committee and in cooperation with all other banks introduced the Nigeria Inter-Bank Settlement System (NIBSS). As stated above, the bank verification number was introduced due to growing incidents of compromise of conservative security systems (PIN and password) and an increased demand in the Nigerian banking system for sophisticated security for sensitive information. The aim of the bank verification number was to protect banks' customers from identity theft and other financial frauds emanating from the Nigerian banking industry (Orji, 2015).

Moreover, there are other scientific mechanisms being used in Nigerian banks, such as forensic technological tools for investigation, secret code, token cards, MasterCard SecureCode, smart card authentication, one-time passwords, multi-layer passwords and memorable words, registered phone numbers, biometrics, data encryption, and closed-circuit television (CCTV) security systems. This is substantiated by Wei et al. (2012), who concluded that electronic banking fraud prevention and control focused on fraud prevention software, smart card authentication, one-time passwords and biometric authentication. The authors further testified that biometric technology provides a better authentication technique and improves the security.

5.4.2.4.2 Awareness and Education

Awareness and education form another set of mechanisms for e-banking fraud mitigation. The quantitative respondents agreed that if all the stakeholders are given adequate knowledge of the causes, impacts and consequences of committing fraud through timely access to information by management; organizational learning for fraud prevention; and adequate consumer education on fraud prevention and personal accounting information protection, including effective fraud awareness training and seminars, this would minimize the incidence of fraud. Therefore, while no bank is excluded from the menace of fraud, decisions can be made to prevent the incidence of fraud and alleviate loss. awareness and education should be used to reduce the perpetration of fraud occurrences.

The same methods can be established to mitigate the volume of loss associated with perpetrated fraud. Appropriate education and training of employees and proper awareness among customers of misconceptions connected with frauds are significant for the deterrence and discovery of fraud (George & Jacob,2015).

The level of customer and staff awareness of fraud can be enhanced through information, education and a controlled and secure environment that helps the detection and prevention of fraud. Not only staff but also customers must be aware of what constitutes fraud incidence and able to recognize risk conditions or factors that are associated with fraud. However, insiders that involved in fraudulent acts must acknowledge and understand the consequences or penalties, including disciplinary actions associated with the perpetration of such acts. Acknowledging and understanding that consequences will be forthcoming would serve as a significant deterrence to fraudulent acts. Therefore, financial institutions have to customer education and training on how to guard against fraud and how to protect their accounts. For instance, respondents reported that banks have been encouraged by the central bank to establish seminars and training for their customers and to use, handbills, leaflets, magazines, media systems and customer care desks for the prevention of frauds.

5.4.2.4.3 Internal Control Mechanisms

Internal control mechanisms form another way of preventing fraud from occurring. Respondents opined that customer screening and employee background checks, automated address verification service and automated phone calls, fraud internal control structures, intelligence gathering systems and clearly defined reporting structures, effective governance, and risk and compliance programmes greatly contributed to the reduction of e-banking fraud in the Nigerian economy. This backs up the view of Bhasin (2016) that one of the most significant insecurity factors organizations encounter is fraud committed by dependable insiders and customers. Banks must perform background verification on prospective employees and customers, and honest testing is required from the organization itself to strengthen its internal controls.

5.4.2.4.4 Legal and Synergies Mechanisms

Legal and synergies mechanisms call for compliance with law and organization policy and mitigation of fraud through the joint effort of the law enforcement forces and other concerned organizations. The survey respondents agreed that e-banking fraud incidents were reduced by effective fraud control policies, regulation, effective corporate codes of conduct, prosecution, availability of effective whistle-blower hotline policies, and collaboration with government regulators, law enforcement agencies and academics. Most of the respondents affirmed that their banks have a written corporate code of conduct and organizational policy to prevent unethical behaviour among the stakeholders, and that their banks give zero tolerance to unethical behaviour.

The survey respondents believed that there is not enough cooperation among the banks in sharing of information, which has created problems in preventing fraud. Therefore, to have effective prevention of fraud, there must be a cordial relationship among the banks, and policies and procedures for sharing fraud incidences and methods of preventing frauds. There should be forums and conferences where fraud incidences and methods for controlling them can be discussed among the banks. As reported by the respondents that, there is the Nigeria Inter-Bank Settlement System, which performs a similar duty in Nigeria. This company has contributed immensely to prevention of e-banking fraud in Nigeria. Furthermore, in the effective prevention of fraud through system technology, people are more important, as there will be effective structures and policy statements when the right personnel are in place

5.4.3 Factor Analysis of the Detection Mechanism

Research Question 4. What are the current significant fraud detection mechanisms for e-banking fraud in the Nigerian banking industry?

5.4.3.1 Assessment of the suitability of the Constructs of Detection Mechanism

Have considered the sample size required for factor analysis as stated in section 4.6. 165 samples were used for this study, which is large enough as suggested that the sample size

for factor analysis must, not less than 100 samples, 150 samples are moderate, and 300 samples are large enough. Pallant (2005; Tabachnick & Fidell, 2007). The coefficient of the correlation matrix is greater than 0.3 which is in line as recommended by Tabachnick & Fidell, (2007) that to determine the strong point of the inter-correlations of the variables, the coefficient of correlation matrix must 0.3 or less. Therefore, the data or constructs are suitable for the factor analysis. Furthermore, to examine the factorability of the constructs or data, two statistical fits were generated which are the Kaiser-Meyer-Olkin (KMO) and Bartlett's of sphericity.

The Kaiser-Meyer-Olkin (KMO) examines the variables' adequacy and factorability with the threshold between 0.7 and 0.9 as strongly acceptable or highly satisfactory (Schumacker & Lomax, 2004). For this study, the KMO measure is 0.764 which is far above 0.6 the minimum value. Therefore, the variables are strongly satisfactory, adequate and dependable for factor analysis. While, the Bartlett's Test of Sphericity for the study is significant ($P<.05$) and appropriate for the factor analysis. Therefore, the constructs for the examination of detection mechanisms of e-banking fraud in this study are appropriate and suitable.

5.4.3.2 Total Variance Explained

Communalities were also reviewed; these disclose the extent of variance in the variables considered for the extracted factors. As seen in Appendix 8, over 95% of the variance in the variables was accounted for by the extraction of the latent variables. This was achieved after excluding all the variables that had extraction values below 0.3.

Table 5.18: Total Variance Explained

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	4.125	22.915	22.915	4.125	22.915	22.915	3.498	19.435	19.435
2	3.457	19.205	42.120	3.457	19.205	42.120	3.116	17.310	36.745
3	2.342	13.009	55.129	2.342	13.009	55.129	2.900	16.113	52.858
4	1.403	7.795	62.925	1.403	7.795	62.925	1.812	10.066	62.925
5	.911	5.060	67.985						
6	.850	4.725	72.710						
7	.761	4.229	76.939						
8	.693	3.849	80.788						
9	.623	3.464	84.252						
10	.570	3.169	87.421						
11	.462	2.566	89.987						
12	.442	2.458	92.445						
13	.416	2.309	94.754						
14	.361	2.004	96.757						
15	.254	1.409	98.167						
16	.187	1.040	99.206						
17	.078	.434	99.640						
18	.065	.360	100.000						

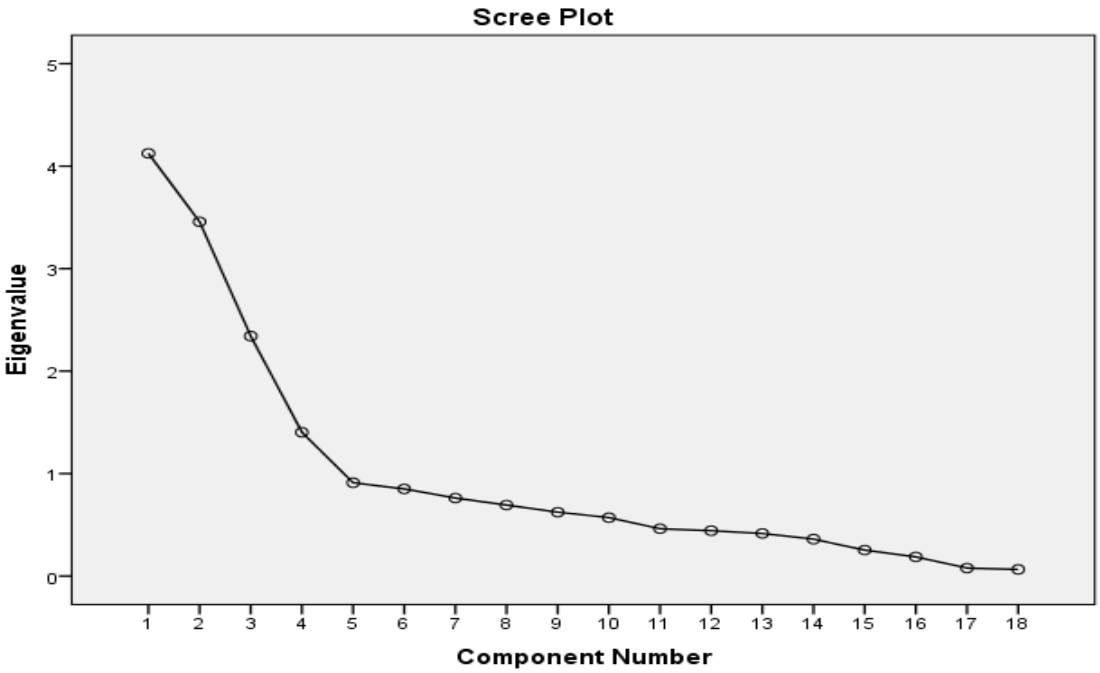
Extraction Method: Principal Component Analysis.

The eigenvalue reflects the number of extracted factors which amount to equal to the number of items that are accounted for in factor analysis. Table 5.18 shows all the extracted factors for the analysis together with their eigenvalues. The eigenvalue table has been grouped into specific sections: initial eigenvalues, extraction sums of squared loadings and rotation of sums of squared loadings. But for the benefit of analysis and interpretation, the researcher was only concerned with extraction sums of squared loadings. The total variance explained table is used to determine the number of factors to extract which meet the criterion or have an eigenvalue of 1 or more. In this case, the first four factors recorded eigenvalues greater than 1 (4.125, 3.457, 2.342 and 1.403; see Total column of initial eigenvalues in Table 5.18. These four factors explain a total of 62.985% of the variance. However, to determine the number of factors to retain out of the four with

eigenvalues greater than 1, parallel analysis was adopted (see Appendix 9) and supported by scree plot (Figure 5.12).

Systematically, the first eigenvalue obtained from principal component analysis (PCA) in SPSS was compared with the equivalent first result from the random values obtained from parallel analysis. The factor was retained if the eigenvalue from PCA in SPSS was greater than the criterion result from parallel analysis; if it was otherwise, the factor was rejected. The results show that the first four factors, with recorded eigenvalues of 4.125, 3.457, 2.342 and 1.403, were accepted and retained (Table 5.18). These four factors explain a total of 62.985% of the variance, with corresponding extraction sums of squared loadings totalling 62.985%. This cumulative variance is highly significant and meets with the threshold of greater than 60%. The remaining factors accounted for a cumulative 37.015% of the variance (Table 5.18), which is insignificant.

Figure 5.12 Scree Plot of the Detection Mechanism



Finally, the rotated component matrix (RCM) was used to present the loadings of each of the cases in the four components as stated above. It could be observed that most of the

cases loaded strongly on the first and third factors, while the second and fourth factors were also well loaded but not as strongly as the first and third components; the researcher programmed SPSS to select only four factors (Appendix 10). This corroborates the earlier conclusion and recommendation from the Monte Carlo PCA for parallel analysis (Appendix 9) and scree plot (Figure 5.12) to extract and retain only the first four factors with eigenvalues of greater than 1. The factors loaded with measured variables which is the outcome of the factor analysis of the perceived mechanisms for the e-banking detection in Nigerian banking industry are summarised below along with their variables and symbols used to represent them in SPSS and at where confirmatory analysis commenced (see Table 5.19).

Table 5.19: Detection Mechanisms of E-Banking Fraud

S/N	Components/ Factors	Loaded Variables	Symbols
1	Technical Mechanisms	Implementation of banking verification number (BVN) approach.	GB1
		Application of automated data analysis and intrusion detection system (IDS).	GB2
		Use of transaction monitoring software.	GB3
		Application of internet banking fraud detection and data mining.	GB4
		Application of forensic computer software and fraud risk assessment and investigation systems.	GB5
		Application of credit card fraud detection tools (Hidden Markov, Parallel Granular and Neural Networks).	GB6
		Application of Hidden Markov.	GB7
		Application of Dynamic Key Generation and Group Key.	GB8
2	Internal Control and Moni	Fraud detection and monitoring systems.	GB9
		Monitoring the internet to detect and close malware websites.	GB10
		Fraud Controls, monitoring and analysis teams.	GB11
		Monitoring phishing-related websites.	GB12
3	Stakeholder's complain an	Customers' complaints.	GB13
		Internal and external whistle-blowers.	GB14
		Anonymous complaints.	GB15
4	Surveillance Mechanisms	Use of CCTV at point of transaction.	GB16
		Internal surveillance equipment.	GB17
		ATM monitoring surveillance.	GB18

Moreover, the next section further tests the relationship between the latent factors and their correspondence observed variables stated in the above Table 5.19 by the use of confirmatory factor analysis.

5.4.3.3 Confirmatory Factor Analysis of the Detection Mechanisms

This section validates the result of the exploratory factor analysis in the Table 5.19 through the testing and verifying the hypothesis that, there is existing relationship between the underlying factors (latent variable) and observed variables in this Table 5.19.

5.4.3.3.1 Reliability and Validity of the Prevention Mechanism Constructs

To ascertain the consistency of the respondents' responses given to 18 items produced by EFA, a reliability test was required. Cronbach's Alpha (α) with coefficient values between 0 to 1 was also employed to determine the interconnectedness of the responses (Saunders et al., 2012; Tavakol & Dennick, 2011).

A total of 165 respondents' responses were considered useable for the 18 items to assess the significant impacts of detection mechanisms on e-banking fraud. Tests of reliability carried out on the constructs gave a Cronbach's Alpha (α) coefficient value of 0.781. This reliability value is greater than the 0.60 minimum threshold of internal consistency (Nunnaly & Bernstein, 1997). The means, the constructs used for the preventive mechanisms of e-banking fraud are valid and reliable for the confirmatory factor analysis.

5.4.3.3.2 CFA Model of the Detection Mechanisms of E-banking Fraud

Confirmatory factor analysis was employed to examine current fraud detection mechanisms that have significant impacts on e-banking fraud detection in Nigerian banks". Before assessing the fit of the structural model, it is essential to present a measurement model to confirm these 18 measured indicators written to reflect the 4 latent variables in the Table 5.19. However, Figure 5.13 below presents the constructed measurement model, which displays loaded factors and estimated items. Items are

permitted to load on only one construct without cross-loading and latent variables are permitted to correlate by using Amos SPSS. There are 4 latent variables with 18 measured variables in the model (Four-factor model): Technical Mechanisms (TM); Internal Control and Monitoring Mechanisms (ICMM); Stakeholders' Complaints and Whistle-Blowers Mechanisms (SCWM) and Surveillance Mechanisms (SM) with their correspondence observed variables.

Furthermore, each of these 18 measurement indicators/variables has a related error term identified as (er) and the output model unveils the associated standardized regression weights between the underlying latent factors or variables and observed indicators or variables (See Figure 5.13).

Typically, the four-factor model precisely hypothesized current mechanisms for e-banking fraud detection in Nigerian banks. These factors are also known as unobserved or latent variables which determine the correlation among the 18 observed or measured variables. The double-edged arrows among the four factors designate that the researcher presumed that these unobserved variables are correlated and the arrows between the latent factors and the observed variables signify factor loadings or linear regression coefficients.

Figure 5.13 Confirmatory Model of Detection Mechanisms

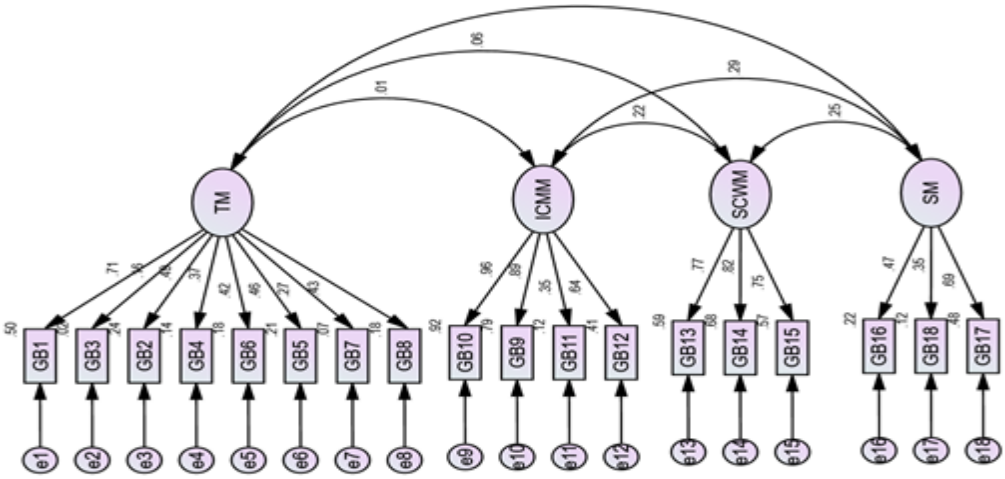


Figure 5.13 presents the observed or endogenous variables are GB1, GB2, GB3, GB5, GB4, GB6, GB7, GB8, GB9, GB10, GB11, GB12. GB13, GBB14, GB15, GB16, GB17 and GB18, while the unobserved or exogenous variables are e1, TM, e2, e3, e4, e5, e6, e7, ICMN, e8, e9, e10, SCWM, e11, e12, e13, e14, e15, e16, SM e17 and e18.

In addition, each of these 18 measurement indicators variables has a related error term identified as (er); the output model unveils the associated standardized regression weights between the underlying latent factors and observed variables (See Figure 5.13). Also, the standard picture in the program Amos makes it clear that the errors are also unobserved factors. Therefore, the total number of variables in the model (Figure 5.13) is therefore 40, which comprises 18 observed or endogenous variables and 22 unobserved or exogenous variables.

The four-factor model in Figure 5.13 has parameters of 18 observed or measured variables. The number of variance sample moments in variance-covariance matrix is 171 which therefor is11(p(p+1))/2= ((18(18+1))/2 = 342/2= 171(Figure 5.13). A saturated model of all paths is 171 + 18 = 189 which means (p(p+3))/2= (18(18+3))/2= 189 free parameters that could be estimated. However, in Figure 5.13 above 42 (6 factor covariance, 18 variable error covariance and 18 factor loadings) parameters would be assessed. The degree of freedom for the four-factor model is hence df = 171 – 42 = 129 (Figure 5.13). The hypothesized model seems to be plausible and a good fit to the data therefore the researcher did not conduct modification model as the following criterion prove the good fit of the data to the model.

Table 5.20: CFA Measure of FIT of Detection Mechanisms

Amos Fit Measures				
Fit Measure	Default	Saturated	Independe	Macro
Number of parameters	42	171	18	NPAR
Discrepancy	84.88	0.000	732.085	CMIN
Degrees of freedom (*df*)	129	0	153	DFR
probability of discrepancy (*P*)	0.999		0.000	P
Discrepancy divided by degrees of freedom	0.658		4.785	CMIN/DF
RMR	0.040	0.000	0.168	RMR
GFI	0.947	1.000	0.648	GFI
Adjusted GFI (AGFI)	0.93		0.607	AGFI
Parsimony-adjusted GFI (PGFI)	0.714		0.508	PGFI
Normed fit index	0.884	1.000	0.000	NFI
Relative fit index	0.862		0.000	RFI
Incremental fit index	1.073	1.000	0.000	IFI
Tucker-Lewis index	1.090		0.000	TLI
Comparative fit index	1.000	1.000	0.000	CFI
Parsimony ratio	0.843	0.000	1.000	PRATIO
Parsimony-adjusted NFI	0.745	0.000	0.000	PNFI
Parsimony-adjusted CFI	0.843	0.000	0.000	PCFI
Noncentrality parameter	0.000	0.000	579.085	NCP
NCP lower bound	0.000	0.000	498.579	NCPLO
NCP higher bound	0.000	0.000	667.116	NCPHI
FMIN	0.518	0.000	4.464	FMIN
F0	0.000	0.000	3.531	FO
F0 lower bound	0.000	0.000	3.04	F0LO
F0 upper bound	0.000	0.000	4.068	F0HI
RMSEA	0.000		0.52	RMSEA
RMSEA lowere bound	0.000		0.141	RMSEALO
RMSEA upper bound	0.000		0.163	RMSEAHI
P for test of close fit	1.000		0.000	PCLOSE
Akaike information criterion (AIC)	168.88	342.000	768.085	AIC
Browne-Cudeck criterion	179.887	386.814	772.802	BCC
Bayes information criterion	299.33	873.117	823.992	BIC
Consistent AIC	341.33	1044.117	841.992	CAIC
Expected cross-validation index	1.030	2.085	4.683	ECVI
ECVI lower bound	1.299	2.085	4.193	ECVILO
ECVI upper bound	1.299	2.085	5.220	ECVIHI
MECVI	1.097	2.359	4.712	MECVI
Hoelter .05 index	303		41	H.05
Hoelter .01 index	328		45	H.01

5.4.3.3.3 Interpretation of the Model Fit of Prevention Mechanisms

The chi-square goodness-of-fit test value is 84.880 with df = 129 and p = 0.999 > 0.05(Table 5.20). which is statistically insignificant χ^2 value comparative with the degree of freedom *(df)* indicating that measured variables and estimated variance-covariance data are plausible and fit. Therefore, the four-factor model fits the variance-covariance data properly. In addition, the researcher considered the maximum likelihood chi-square (ML χ^2*)* estimation technique.

The Maximum likelihood chi-square ML χ^2 can also be calculated through minimum fit function value (FMIN) in Table 1 above. The chi-square is χ^2*= (n-1)fm, where "fm"* is the minimum fit function value *and "n"* represents the sample size. The sample size for this model is *165 while FMIN is 0.518 therefore* ML χ^2 = (165 – 1) *0.518* = 84.952(Table 5.20).

Goodness of fit (GFI) model fit criterion ranges from 0, signifying poor, to 1, representing excellent fit. Specifically, value greater than or equal to .95 shows an excellent fit (Schumacker and Lomax, 2004 and Blunch, 2013). Thus, in the Table 5.20, the GFI value of 0.947 indicating of a better fit. It is therefore concluded that the latent factors and observed variables in this present study fits the model properly.

The Goodness of fit (GFI) index is this model analysis is 0.947(Table 5.20). Therefore, AGFI index is: 1 – [R/df) (1-GFI)] = 1 – [(171/129) (1- 0.947)] = 0.930. The model fit scale for Adjusted Goodness of Fit (AGFI) is 0 (poor fit) to 1 (excellent fit). Precisely, value adjusted for degree of freedom with .95 is a satisfactory mode fit (Schumacker and Lomax, 2004). Therefore, 0.930 (Table 5.20) is the AGFI model analysis for this study which indicates that the model is perfectly fit.

The square root of the mean-squared (RMR) for this study is 0.040 (Table 5.20). This indicates that the square root of the inconsistency between the model sample covariance matrix and covariance matrix is very close.

The Root Means Square Error of Approximation (RMSEA) standard scales range from 0 to 1, with lesser values representing better model fit. A range of .05 or less is signifying satisfactory model fit while, range of zero is perfectly fit (Schumacker and Lomax, 2004 and Blunch, 2013). In the current study, the Root Means Square Error of approximation (RMSEA) value for the hypothesized model is 0.000 (Table 5.20) Thus, the model is satisfactorily acceptable and perfectly fit.

Tucker-Lewis Index (TLI) is used to equate alternative models or a projected model against a null model. The TLI range from 0 (no fit) to 1 (perfect fit). Precisely, value greater than or equal to 0.95 reflects a good model fit. The value of TLI for this current study was calculated as $[X^2null/dfnull) - (X^2model/dfmodel)]/[(X^2null/dfnull) - 1] = [(732.082/153) - (84.880/129)] /[(732.085/153) - 1] = 1.090$ (Table 5.20) Therefore, the model for this analysis is fit and satisfactory.

In this analysis, Normed Fit Index was calculated as (731.085 – 84.880)/732.085 = 0.884, the Comparative Fit Index (CFI) for this analysis is 1.000 while, Incremental Fit Index (IFI) and Relative Fit Index (RFI) and are and 1.073 and 0.862 respectively. Therefore, the hypothesized model for this current analysis is perfectly fit because NFI, CFI, RFI and IFI values are greater than 0.7.

Inconclusion, there is correlation between the observed variables and the latent factors which means, Technical Mechanisms (TM), Internal control and monitoring Mechanisms (ICMM), Stakeholder's complain and whistle-blowers Mechanisms (SCWM), Surveillance Mechanisms (SM) are current detective mechanisms of the e-banking frauds detection in Nigerian banking industries.

5.4.3.4 Discussion of the Findings

The outcome the EFA and CFA analyses in section 5.4.3. Makes provision for the method for the detection of e-banking frauds in Nigerian banking institutions which are the following mechanisms: Technical Mechanisms (TM), Internal control and monitoring Mechanisms (ICMM), Stakeholder's complain and whistle-blowers Mechanisms

(SCWM), Surveillance Mechanisms (SM) are current detective mechanisms of the e-banking fraud detection in Nigerian banking industries.

5.4.3.4.1 Technical mechanisms

Technical mechanisms are the methods for deterring and detecting e-banking fraud through electronic systems and software devices. It was reported by the respondents that some frauds had been discovered through the means of the banking verification number approach; automated data analysis; intrusion detection systems (IDS); transaction monitoring software; internet banking fraud detection and data mining; forensic computer software; fraud risk assessments and investigation systems; and credit card fraud detection tools such as Hidden Markov, Dynamic Key Generation and Group Key and Parallel Granular and Neural Networks. These are highly effective tools of fraud detection. Similarly, 75% of the questionnaire respondents agreed that technical mechanisms are effective means of exposing frauds and perpetrators (see Section 5.3.4). George and Jacob (2015) concluded that electronic banking fraud prevention and control should be focused on fraud prevention software, smart card authentication, one-time passwords and biometric authentication. The authors further testified that biometric technology provides a better authentication technique and improves security.

5.4.3.4.2 Internal control and monitoring Mechanisms (ICMM)

The survey respondents consented that monitoring mechanisms are major techniques for detecting e-banking fraud in Nigeria: through fraud detection and monitoring systems, monitoring the internet to detect and close malware websites, fraud controls, and monitoring and analysis teams. Bhasin (2016) stated that one of the most significant insecurity problems organizations encounter is fraud committed by dependable insiders and customers. Human resources department and cash control unity must perform background verifications on prospective employees and customers, and honest testing is required from the organization itself.

5.4.3.4.3 Stakeholder's Complain and Whistle-blowers Mechanisms (SCWM),

The survey respondents revealed that many frauds have been detected through customers' complaints, internal and external whistle-blowers, anonymous complaints and personal confessions. The quantitative analysis of this study showed that 75% of e-banking fraud was detected through fraud hotlines and whistle-blowers (see Section 5.3.4).. This was supported by KPMG (2007) in a study in Africa, the Middle East and Europe, reported 24% of fraud detected through whistle-blowers. This was corroborated by staff preferences for anonymous whistle-blowing or hotline policies rather than open whistle-blowing because the latter leaves the whistle-blower open to insecurity, retaliation and isolated (Dworkin & Baucus, 1998). Therefore, banks need to make policies that will give assurance, adequate security and confidence to the whistle-blower to gain protection through whistle-blowing.

There are other mechanisms of fraud detection, such as recruitment of new employees and staff rotation. Many frauds have been discovered through customer complaints and personal confessions. The respondents confirmed that some of the e-banking frauds that have been discovered were through customers' complaints when they discovered fraudulent withdrawals from their accounts. Therefore, developing a principle or policy that motivates stakeholders who recognize fraudulent incidences to report them to the appropriate quarter through an ethical channel or hotline should be a priority for banks.

5.4.3.4.4 Surveillance Mechanisms

Survey respondents reported that surveillance mechanisms have played a significant role in detecting and discovering e-banking frauds in Nigerian banks. Respondents testified that some frauds, particularly at ATM points, have been detected through CCTV at the point of transaction, internal surveillance equipment, ATM monitoring surveillance, bank security officers and the police. Internal and external surveillance equipment also play significant roles in fraud detection. The respondents also declared that some e-banking frauds had been detected during online accounting reconciliation, management review, and internal and external audit assessments (see Table 5.19 and Section 5.3.4).

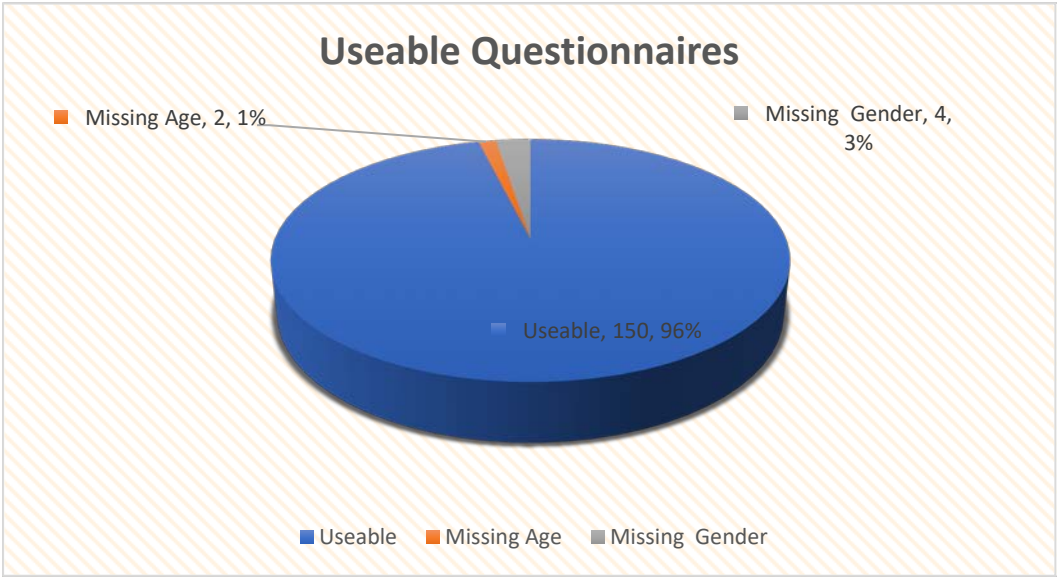
5.5 Analysis of the Customers' Responses

This section presents the analyses of the quantitative data that were collected to evaluate the attitudes of customers to prevention and detection of frauds in their e-banking accounts with Nigerian banks. The section commences with data entry and validation through the examination of the demographic characteristics of the respondents, then

5.5.1 Data Entry and Sorting

A preliminary examination was completed prior to the inferential and descriptive analyses to measure the correctness of the data entry. This was performed in terms of the response rate and the amount of missing and valid cases. The correctness of the data entry was analysed in terms of the number of missing valid cases. In the chat below (Figure 5.14), of all 156 recovered copies of the questionnaire, 156 (100%) were from valid customers. A total of 6 (3.84%) constructs cases were missing and 150 (96.15%) were suitable for analysis. Therefore, the total number of valid copies of questionnaires for this analysis was 150. The excluded copies of questionnaires (the missing cases) are insignificant compared with the total; they were removed.

Figure 5.14: Useable Questionnaires

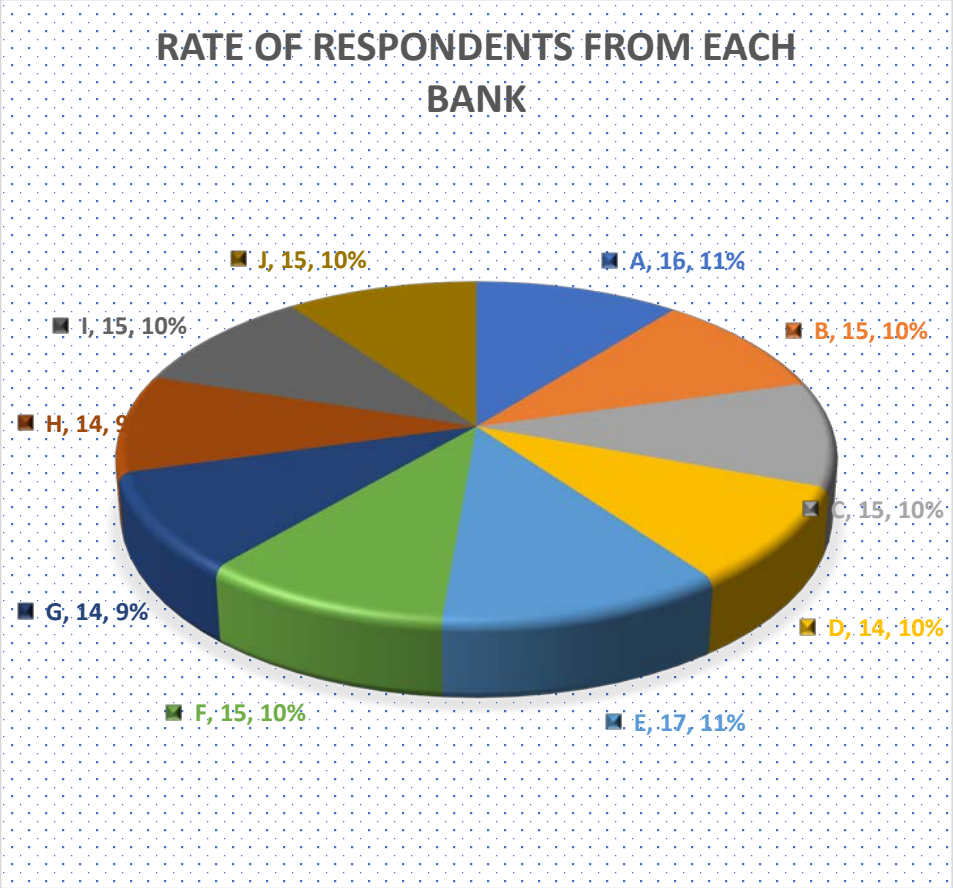


5.5.2 Demographic Analysis

5.5.2.1 Rate of Customers' Responses from Each Bank

Figure 5.15 shows that 17 (11%) of the respondents were customers of Bank E, followed by Bank A (16 (11%)), while banks B, C, F, I and J had the same number of respondents (15 (10%)), and the rest had 14 (9%) respondents apiece. However, there was no serious difference in the distribution analysis of respondents across the selected banks.

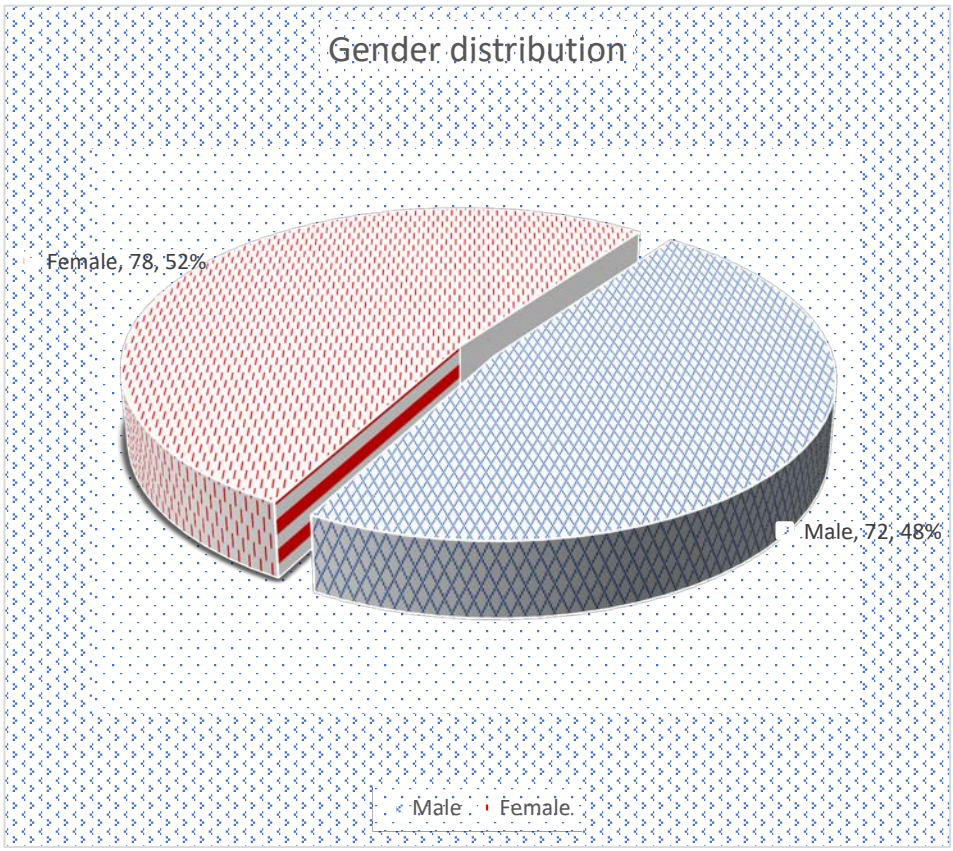
Figure 5.15: Rate of Respondents from Each Bank



5.5.2.2 Gender Distribution of the Respondent Customers

Figure 5.16 presents the gender of the respondents, which reveals that the number of females in the sample was 78 (52%), while the number of males was 72 (48%). Here, there were more female respondents than males. It generally looks as if, for some banks, women dominate their customer base.

Figure 5.16: Gender Distribution

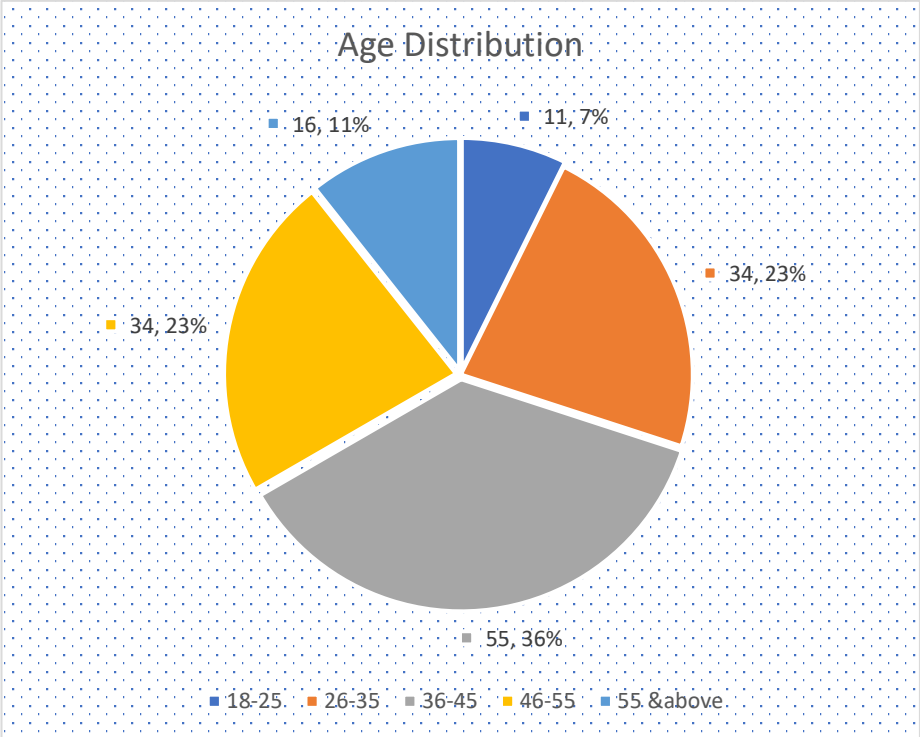


Source: Survey questionnaires

5.5.2.3 Age Distribution of the Respondents

Figure 5.17 presents the age range of the respondents. This reveals that 11 (7.33%) of the respondents were in the age range of 18–25 years, 34 (22.67%) were aged 26–35, 55 (36.67%) were in the range of 36–45 years, 34 (22.67%) were aged 46−55 and 16 (10.67%) were aged 56 years and above. This means that 139 (92.67%) of the respondents were above 25 years old. Hence, the respondents were old enough to have had experience of banking fraud and would have experienced the impact of being defrauded as well as the effects of it on individuals and organizations.

Figure 5.17: Age Distribution

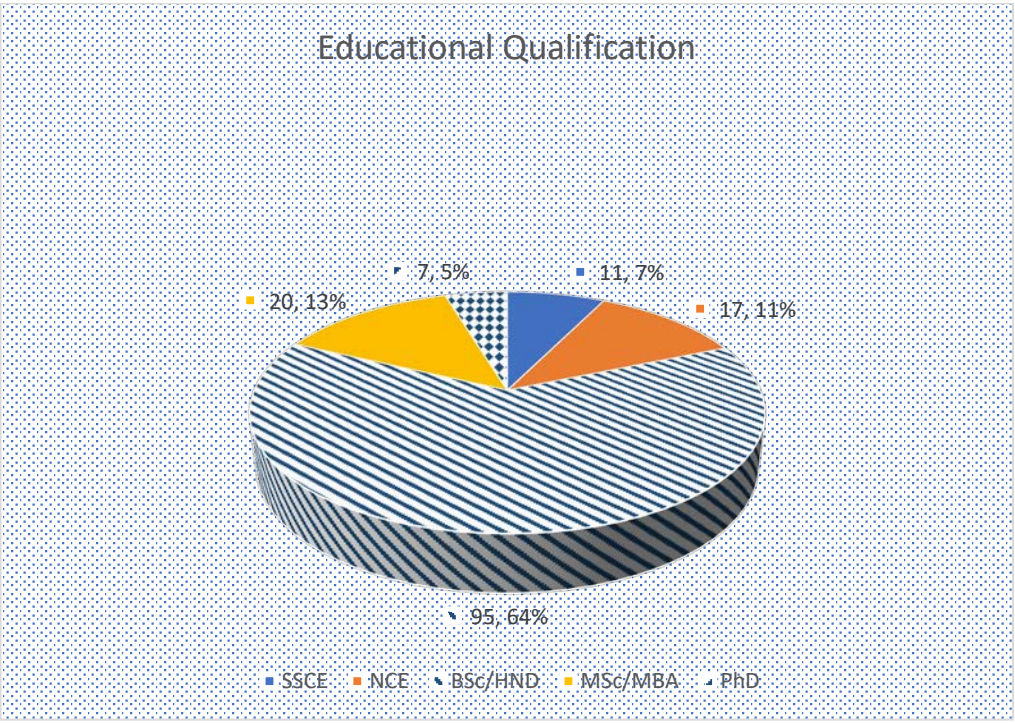


Source: Survey questionnaires

5.5.2.4 Educational Qualification

Figure 5.18 presents the academic qualifications of the respondents. It shows that 5% of the participants had Doctorate degrees, 13% had acquired master's degrees, 64% hold bachelor's degrees, 11% had National College of Education Certificates and the remaining 7% of the respondents had Senior School Certificates. This indicates that all respondents are educated, have knowledge and experience of academic research and its relevance and importance in the academic realm and national economy generally, and have been victims of e-banking fraud. Therefore, the information given would be relevant and reliable to make decisions on the current phenomenon.

Figure 5.18: Educational Qualifications



Source: Survey questionnaires

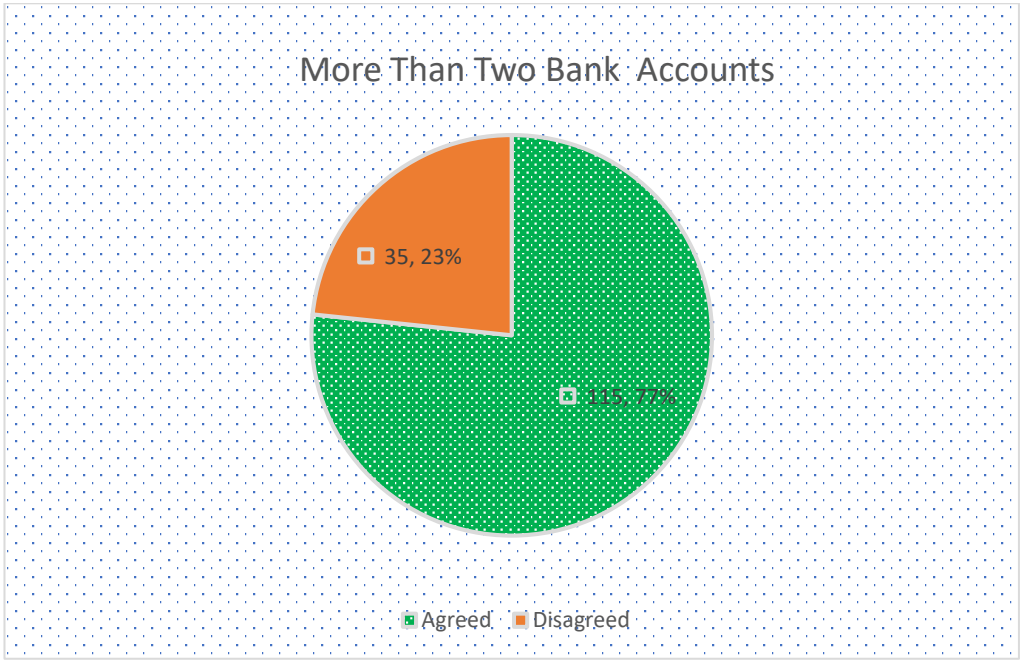
5.5.3. Analyses of the Customers' Responses

This section discusses the attitude and behaviour of Nigerian banks' customers towards prevention and detection of e-banking frauds in Nigeria.

5.5.3.1 Customers Having More Than Two Bank Accounts

Figure 5.19 presents the number of bank accounts owned by each individual respondent. It reveals that out of 150 respondents, 32 (21.3%) had one bank account, 51 (34%) had two bank accounts, 40 (26.67%) had three bank accounts, 18 (12%) had four bank accounts, and 9 (6%) had more than four bank accounts. Precisely 21.33% of the respondents had one bank account while, 78.67% of the respondents had more than one bank account.

Figure 5.19: Customers Having More Than One Bank Account

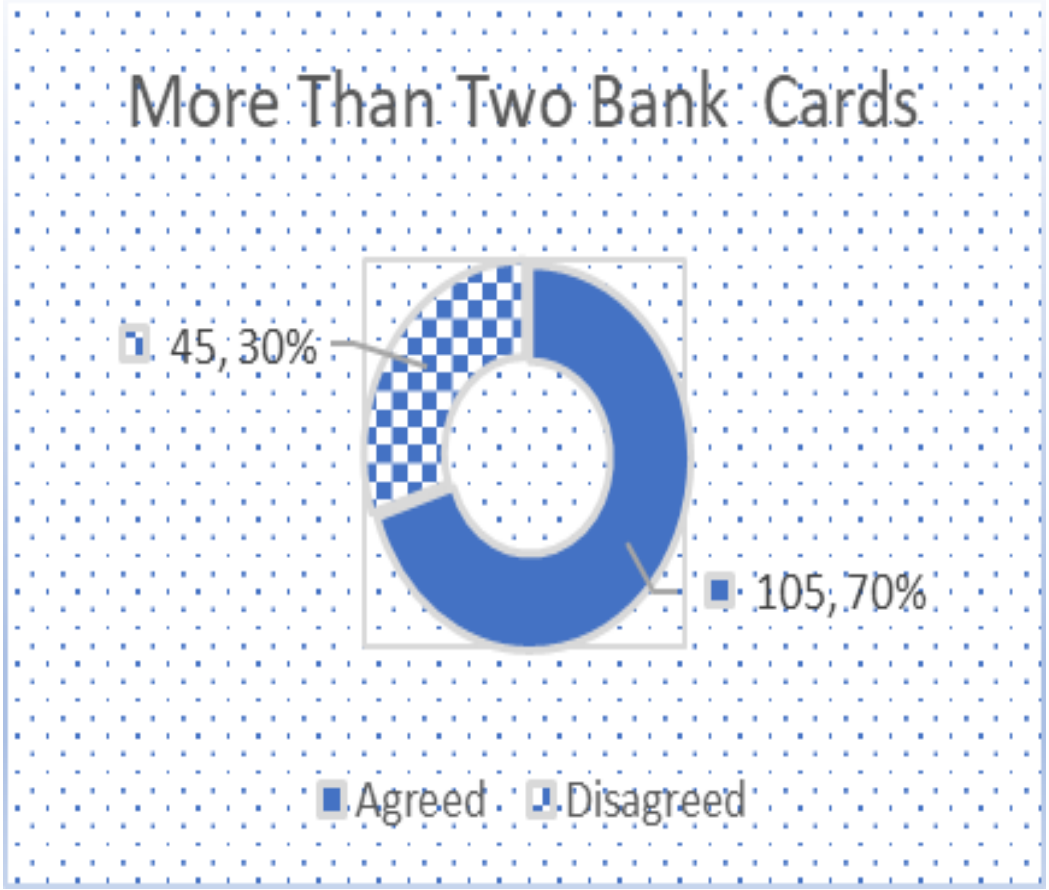


Source: Survey questionnaires

5.5.3.2. Customers Having More Than Two Bank Cards

Figure 5.20 presents the number of bank cards owned by individual respondents. It reveals that out of 150 respondents, 42 (28%) had one bank card, 41 (27.33%) had two bank cards, 35 (23.33%) had three bank cards, 25 (16.6%) had four bank cards, and 7 (4.6%) had more than four bank cards. Exactly 28% of the respondents had one bank card while 72% had more than one bank card.

Figure 5.20: Customers Having More Than One Bank Cards

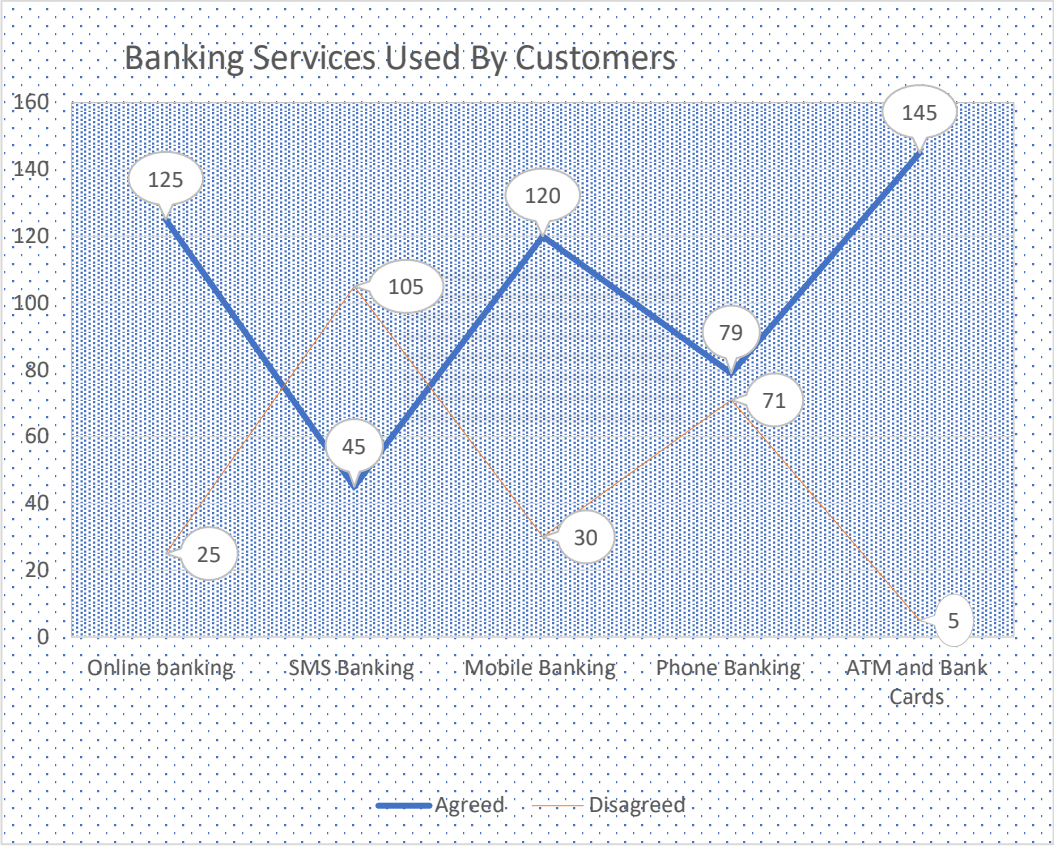


Source: Survey questionnaires

5.5.3.3 Categories of E-Banking Services Individual Customers Use Regularly

Figure 5.21 presents the classes of e-banking services, individual respondents used regularly. It reveals that 42 (28%) of respondents used online banking and e-fund transfer services, 48 (32%) used an ATM and bank card services regularly, 35 (23.33%) used mobile banking services, 18 (12%) used phone banking services and 7 (4.6%) used SMS banking services. Generally, it is obvious that Nigerian banks' customers are using e-banking services regularly; particularly ATM services, bank card services, online banking services, e-fund transfer services and mobile banking services.

Figure 5.21: E-Banking Services Used by Customers

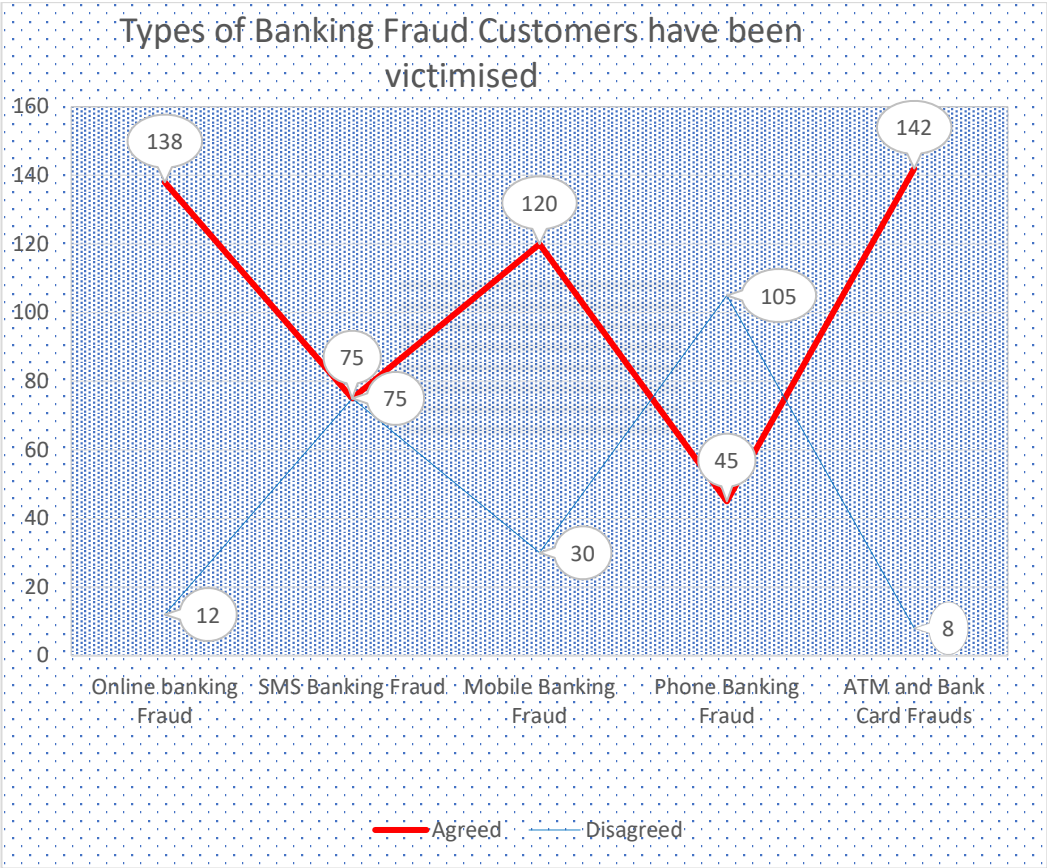


Source: Survey questionnaires

5.5.3.4 Types of E-Banking Fraud Suffered by the Customers

Figure 5.22 presents the types of e-banking fraud suffered by the customers. Out of 150 respondents, 138 respondents stated that they had suffered online banking frauds, 142 agreed that they had suffered ATM and card fund transfer frauds, 120 revealed that they had suffered mobile banking frauds, and 105 agreed that they had suffered phone banking fund transfer frauds. This means that many Nigerian bank customers suffer e-banking frauds. The top three e-banking frauds suffered by the customers are ATM, internet banking and mobile banking frauds.

Figure 5.22: Types of E-banking Fraud, Customers Have Been Victims

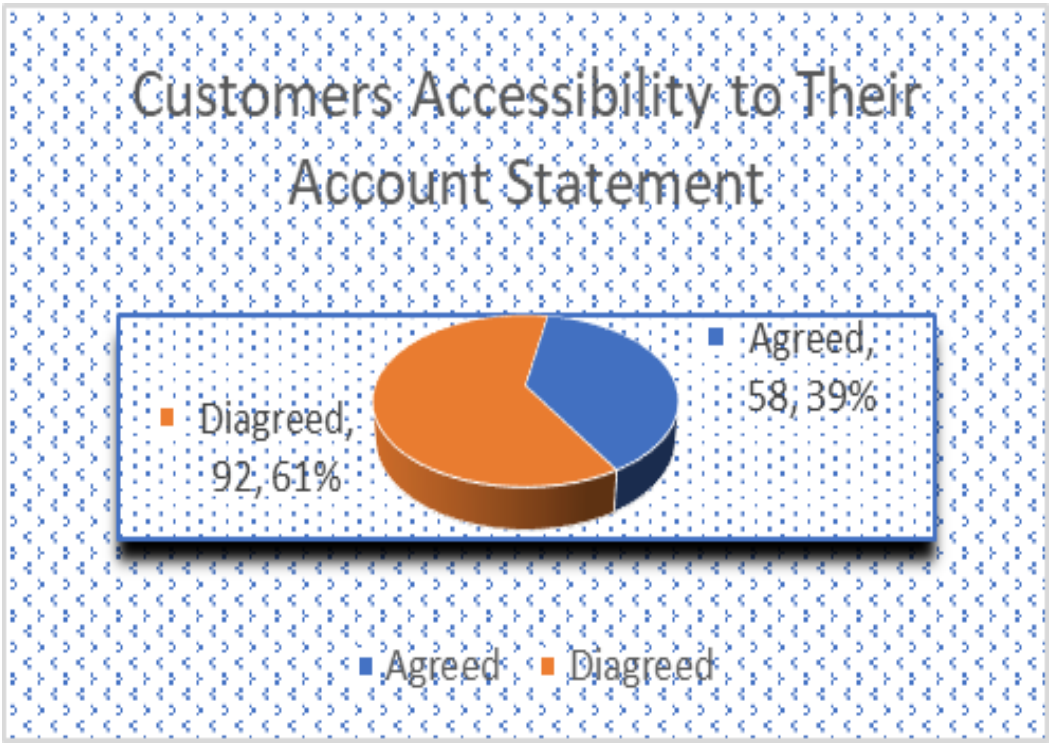


Source: Survey questionnaire.

5.5.3.5 Do Nigerian Banks Regularly Produce Bank Statements for Their Customers?

Figure 5.23 displays how often Nigerian banks make account statements available to their customers. Of the respondents, 92 (61%) believed that their banks did not produce their account statements for them regularly; some even indicated that they had not received a bank account statement at all for more than ten years since they had opened their accounts. Only 58 (39%) agreed that they receive their account statements regularly. This means that Nigerian banks have not made the financial statements of individual customer available to them often enough, which may influence the customers' limited awareness of fraud in their bank accounts.

Figure 5.23: Customers' Access to Account Statements

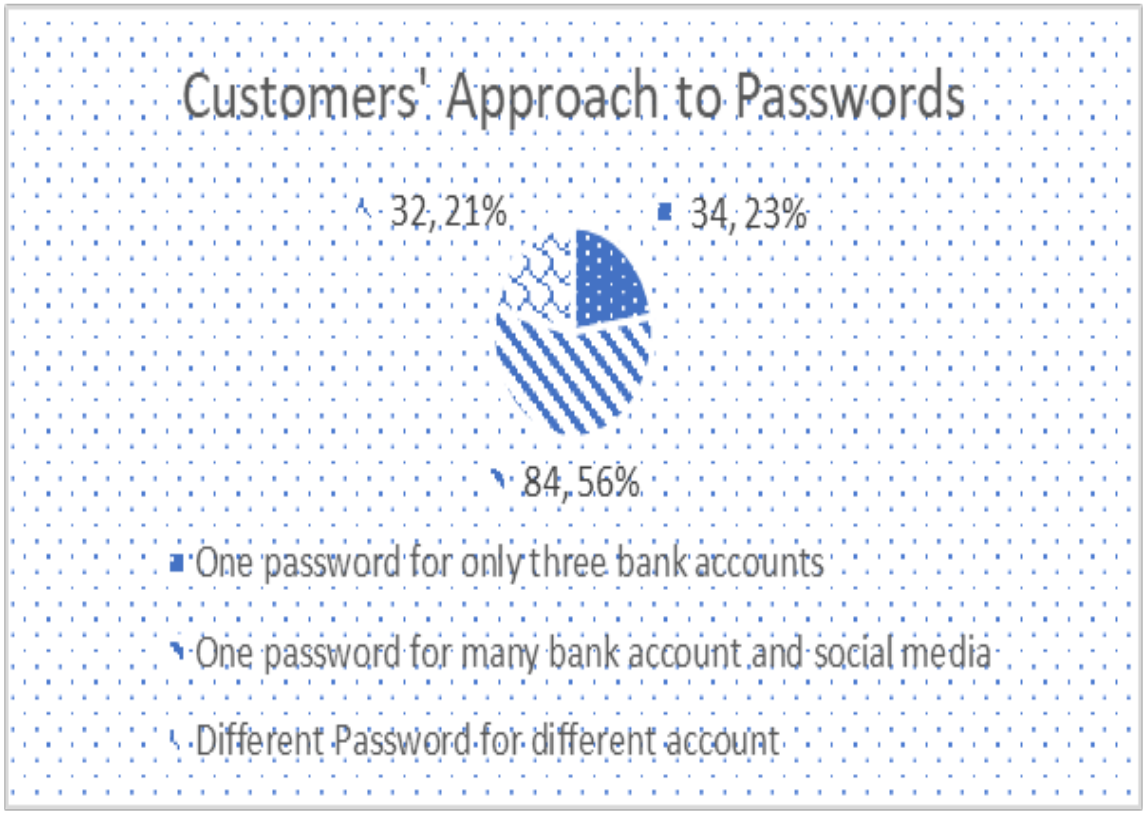


Source: Survey questionnaire

5.5.3.6 Approach to Use of Account Passwords by the Customers

Figure 5.24 reveals how customers used their account password. The investigation disclosed that 34 (22.6%) respondents used one password for three bank accounts, 84 (56.00%) used only one password for many bank accounts and social media, and 32 (21.33%) used different passwords for different bank accounts. This indicates that 79% of Nigerian bank customers' passwords are vulnerable to fraud.

Figure 5.24: Customers' Approach to Passwords

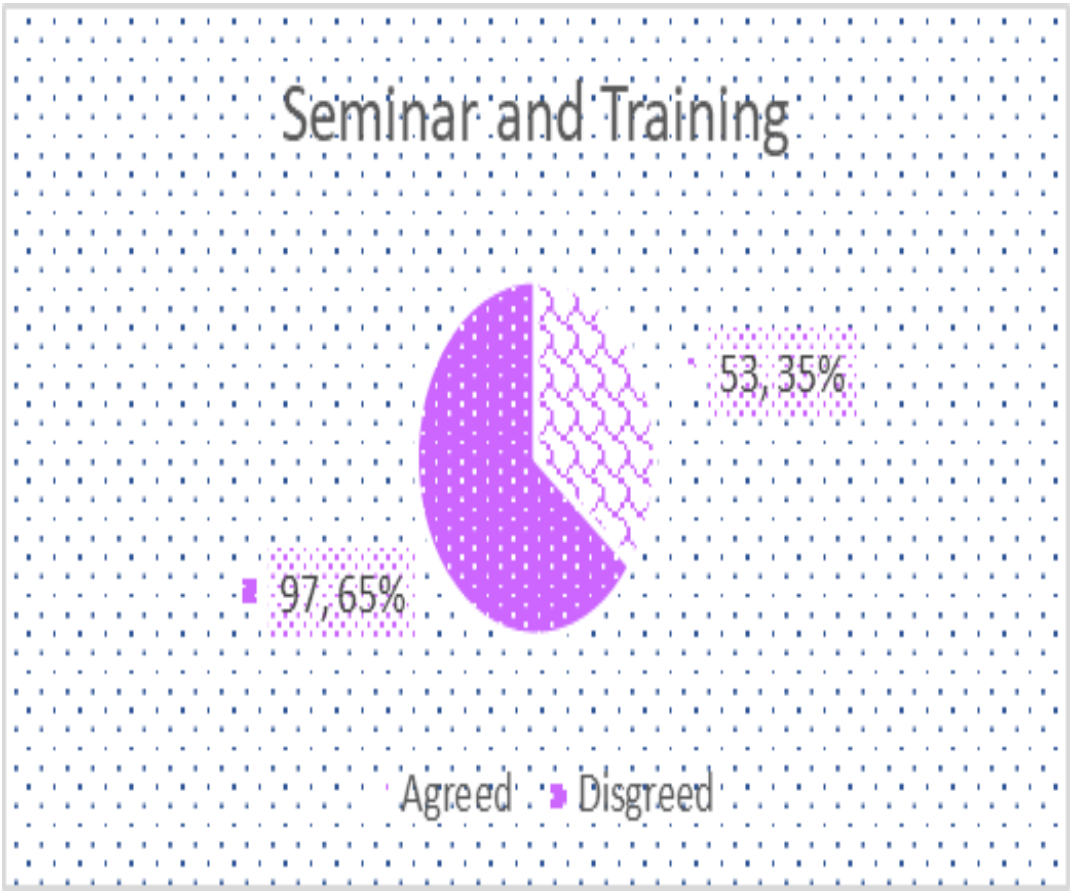


Source: Survey questionnaires

5.5.3.7 E-Banking Fraud Prevention and Detection Seminar/Training

Figure 5.25 presents the outcome of the investigation on the item "Nigerian banks offer e-banking fraud prevention and detection seminar to their customers". It reveals that 53 (35.33%) respondents agreed, while 97 (64.67%) disagreed. This means that Nigerian banks do not provide enough information on fraud and how to prevent it to their customers.

Figure 5.25: Customers' Access to Seminars/Training

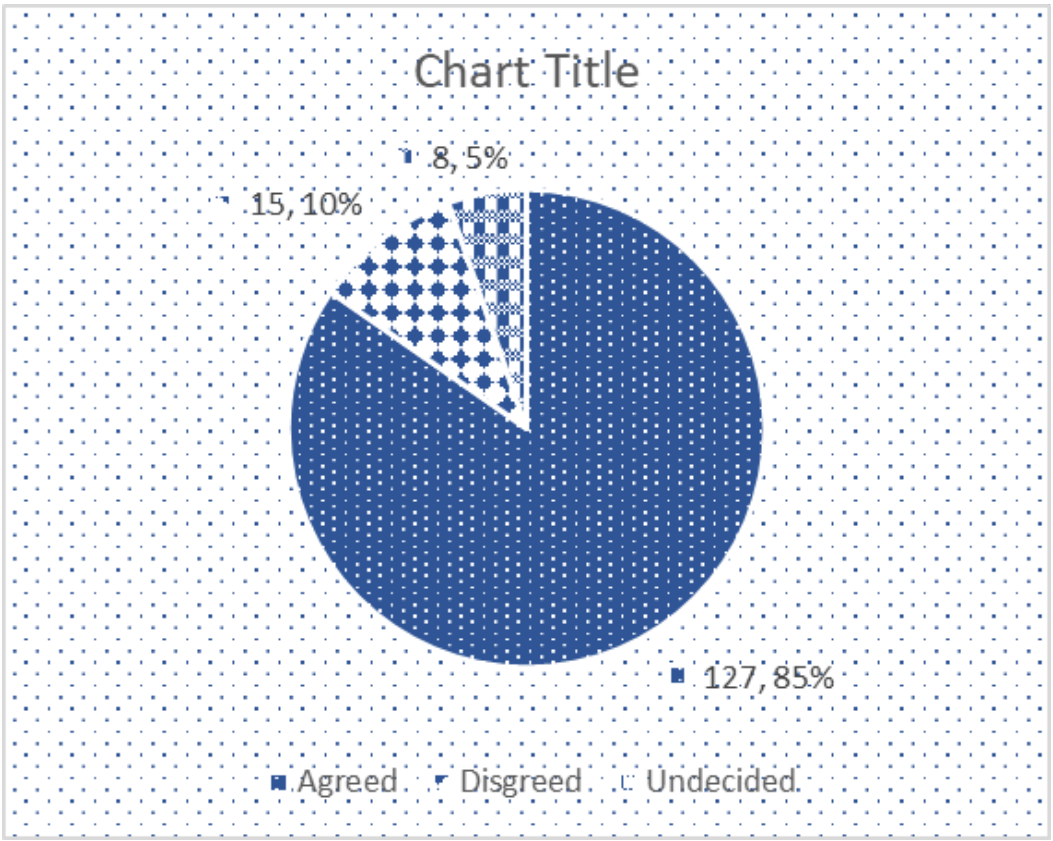


Source: Survey questionnaires

5.5.3.8 Customers' Awareness of E-Banking Fraud Prevention and Detection

Figure 5.26 reveals respondents' opinions on whether customer knowledge of e-banking fraud prevention and detection would have a positive impact in the fight against e-banking fraud in the Nigerian financial institutions. It shows that 127 (84.67%) respondents agreed, while 15 (10%) disagreed and the remaining 8 (5.33%) were undecided. This indicates that Nigerian banks need to create more awareness of e-banking fraud among their customers, and that method of preventing and detecting fraud must be taught by means of seminars and training.

Figure 5.26: Customers' Awareness of E-Banking Fraud



Source: Survey questionnaire.

5.6 Summary

The quantitative analysis of e-banking fraud prevention and detection in Nigerian banks was made with the use of descriptive and inferential analysis (exploratory factor analysis (EFA) and confirmatory factor analysis (CFA) on data from 156 respondents. The analysis has shown the categories of e-banking fraud that are prevalent in the Nigerian banking industry: internet banking frauds, ATM fund transfer frauds, mobile banking frauds and debit/credit card frauds.

The analysis also identified the contributing factors to the increase of these e-banking frauds which are: ineffective banking operations and internal controls, improper banking management, lack of bank staff education and training, lack of sophisticated preventive and detective technological tools, lack of customer awareness, ineffective legislation and law enforcement, inadequate infrastructural and financial resources, economic pressure and presence of sophisticated technological fraudsters, negligence of banks' customers to e-banking account devices and lack of compliance with the banking rules and regulations.

Furthermore, the analysis has made provision for prevention and detection of the occurrence of e-banking fraud in Nigeria. Mechanisms for achieving this were grouped into the following categories: technological mechanisms, legal and synergy mechanisms, awareness and educational mechanisms, surveillance mechanisms, and internal control and whistle-blower mechanisms.

CHAPTER SIX: QUALITATIVE RESEARCH

6.0 Introduction

Based on the research methodology in Chapter 4, this chapter deliberates on the analysis of data collected through the survey interviews. Section 6.1 describes the demographics of the interviewees, while section 6.2 offers a brief elucidation of the analytical tools (that is, thematic analysis and content analysis) chosen for interpreting the face-to-face interviews conducted with ten corporate executives of selected commercial banks in Nigeria. Section 6.3 concentrates on the discussion and presentation of the analysed data, including validation of the research hypotheses regarding the evolving findings. Section 6.4 completes the chapter with a summary of all the issues discussed.

6.1 The Demographics of the Interviewees

The demographics of the interviewees from ten selected Nigerian banks are represented in Table 6.1 below.

Table 6.1: Demographics of the Interviewees from Selected Nigerian Banks

S/N	Bank	Department	Length of Ti	Position	Gender
1	A	Banking and Payment System Department	7 years	Manager	Male
2	B	Nigeria Automated Clearing System (NACS) Department	6 years	Team Head	Male
3	C	Treasury and Forex Management	6 years	Manager	Male
4	D	Operational Risk Management	5 years	Manager	Male
5	E	Inspection and Audit	4 years	Team Leader	Male
6	F	Information and Monitoring Technology	6 years	Team Leader	Female
7	G	Fraud and Investigation Department	4 years	Senior Staff	Female
8	H	Operation and Information Technology	6 years	Manager	Male
9	I	Business Continuity Management	7 years	Manager	Female
10	J	Risk Management	4 years	Manager	Male

Source: Interview (2017)

6.2 Analytical Tools for the Interviews

For the qualitative research, ten executives from deposit money banks (DMBs) (commercial banks) were interviewed between on the 14th April and 26th May 2017. The face-to-face interviews were enriched by personal jottings on vital points emphasized by the interviewees. After the conclusion of the interview meetings, the raw interview responses were methodically transliterated using thematic analysis (TA) and content analysis (CA) collectively. Both are extensively used methods for analysing open-ended questions or qualitative data. Each of the two techniques by itself is sufficient for research, but this thesis amalgamated both analytical tools for strength and robustness of the analysis. Succinct differences between thematic analysis (TA) and content analysis (CA) are elucidated in the subsequent sections.

6.2.1 Content Analyses

Content analysis (CA) is a systematic and analytical tool adopted by researchers in the direction of interpretivists for compressing, summarizing, classifying and tabulating large volumes of words of text into fewer content classes to make the data memorable, meaningful and suitable for decision-making (Saunders et al., 2012; Stemler, 2001; Horn, 2010). Harwood and Garry (2003) described CA as an extensively used technique for analysing the content of a diversity of data, particularly verbal and visual data. Applications have been discovered for CA for both quantitative and qualitative data, contrary to the commonly-held view that it is only used to process qualitative data (Collins & Hussey, 2009).

CA has higher and lower levels: interpretative and descriptive data. The descriptive level of content analysis is the precise quotation of what the participants or interviewees said without the contributions or inputs of the researcher, while the interpretative or

explanatory level is what is intended by the quotations; specifically, the inference or interpretation drawn by the investigator (researcher) (Saunders et al., 2012).

Denscombe (2010) opines that content analysis is a systematic technique for measuring the contents of writings, texts, pictures, speeches, voices, correspondence, books, interviews and other verbal data. It can also be defined as a tool or technique for analysing interview transcripts or open-ended questions or to govern the frequency and presence of certain concepts, words and refrains based on which inferences and meanings are made (Horn, 20010).

Content analysis depends on coding and categorizing of data in chronological demeanours. Before using content analysis in research, the researcher must recognize the typologies of CA. This is essential to have a valid assumption or inference. Content analysis is classified into six varieties: semantic analysis, pragmatic analysis, designation analysis, assertions analysis, sign-vehicle analysis and attribution analysis (Harwood & Garry, 2003). The connotations of the recognized typologies are enhanced and explained in Table 6.1 below.

Table 6.2: Typologies of Content Analysis

S/N	Typology	Explanation
1	Pragmatic analysis	This explores cause-effect associations among contents, ideas and words in terms of impact and frequency.
2	Semantic analysis	This observes the critical meanings of words within the vocal sound or speech and documented data and their occurrence in the subject being examined.
3	Designation analysis	This analysis the occurrence of references to a person, thing, object, word, theme in a piece or article.
4	Attribution analysis	This explores the frequency of descriptions connected to positive attributes.
5	Sign-vehicle analysis	This observes the frequency of convincing utterances in a speech or text.
6	Assertions analysis	This analysis the frequency of attributes associated with an object.

Source: Harwood and Garry (2003, p.481); Raimi (2015).

6.2.2 Thematic Analysis (TA)

Thematic analysis is another globally used analytical technique in qualitative research, particularly for textual data and analysing interviews. Thematic analysis has been defined in several ways. For Braun and Clarke (2014), thematic analysis is a tool in qualitative analysis for recognizing underlying assumptions, conceptualization of interviews, identifying ideas, categorizing texts, open-ended feedbacks, analysing data and reporting the patterns and themes that develop from the data; these authors further state that thematic analysis is adopted by realists and interpretivists to report their knowledge and meanings given to social reality. Valsmoradi, Turunen and, thematic (2013) analysis is a type of pattern or model analysis, through which emergent codes and themes are identified based on perceptions from grounded theory. The connotations and meanings deduced from patterns and themes in qualitative research could be acknowledged through an inductive approach or through the deductive approach (Dures et al.2011). While, Horn, Braun & Clarke, (2006) said that thematic analysis drives forward to interpret several sub-themes or aspects of the themes that develop after coding and transcription of raw data.

Table 6.3: Stages in Good Thematic Analysis

SN	Typology	Explanation
1	Pragmatic analysis	This explores cause-effect associations among contents,
		ideas and words in terms of impact and frequency.
2	Semantic analysis	This observes the critical meanings of words within the vocal sound or speech
		and documented data and their occurrence in the subject being examined.
3	Designation analysis	This analysis the occurrence of references to a person,
		thing, object, word, theme in a piece or article.
4	Attribution analysis	This explores the frequency of descriptions connected to positive attributes.
5	Sign-vehicle analysis	This observes the frequency of convincing utterances in a speech or text.
6	Assertions analysis	This analyses the frequency of attributes 'associated with an object.

Source: Braun and Clarke 2006 (2006, p.37); Raimi (2015).

The chronological stages contained in thematic analysis are as follows. Stage one, the researchers familiarise and relate themselves properly with the data. Stage two, identification and generation of preliminary categories or codes. Stage three, exploration of common themes; review, read and modify the themes when enhanced insights have grown from the data. Stage four, modifying and naming or titling of themes. Stage five, provision of the final report on which conclusions will be based (Saunders et al., 2012, Denscombe, 2010; Horn, Braun & Clarke, 2006). These five stages above were methodically observed while analysing the voice data collected from the interviews conducted with the senior staff from the Nigerian Deposit Money Banks (DMBs). This thesis has a total of five research questions and all research questions were covered by the interviews, which by design is an exploratory technique. However, there are 5 themes and 23 sub-themes with several related significant issues (codes). The themes are nature of e-banking frauds, impacts of e-banking frauds, contributing factors of e-banking frauds, preventive mechanisms of e-banking frauds and detection mechanisms of e-banking frauds.

6.3 Analysis of Interviewees' Responses

The first theme is the nature of e-banking fraud, with four sub-themes: automated teller machine (ATM) frauds, mobile and telephone banking frauds, debit/credit card frauds and internet banking frauds (see Table 6.4). The second theme, contributing factors of e-banking fraud, includes seven sub-themes: operational factors, managerial factors, educational factors, technological factors, legal factors, infrastructural and financial factors, and personnel factors. The third theme, preventive mechanisms of e-banking fraud, has five sub-themes: scientific mechanisms, legal and synergies mechanisms, awareness and education mechanisms, surveillance mechanisms, and internal control mechanisms. The last theme, detection mechanisms of e-banking fraud, has five sub-themes: technical mechanisms, monitoring mechanisms, whistle-blower mechanisms, surveillance mechanisms, and management protocol. The views of the interviewees related to these themes are discussed extensively in the next section.

6.3.1 Nature of E-Banking Fraud in Nigeria.

The nature of e-banking fraud in Nigeria was identified through the responses of the respondents to this interview question: "Since when you have been working in the bank, have you observed any e-banking fraud incident in last three years and what are the kinds of fraud you observed currently?" The aim of this was also to answer research question one: "What are the e-banking fraud risks that are of high concern in the Nigerian banking sector?" In the semi-structured interviews, the researcher searched for the viewpoints of ten senior staff of the selected Nigerian banks on this perception and related issues. Here are the responses, followed by the analysis and discussion.

> *"Yes, almost all of the e-banking frauds we have been experienced in this bank since 2010 can be categorized as ATM and POS frauds. These occurred at the point of ATM fund transaction while some legitimate card owners gave their bank cards to a criminal with the aims of assisting them to operate the machine without knowing that so-called criminal would defraud them. Apart from internet and ATM frauds through identity theft and phishing, recently e-banking crime was observed when fraudsters installed hardware in the bank branch systems to manipulate financial transactions via mobile network e-fund transfer.*" (Bank A: Interview, 2017).

> *"Yes, e-banking fraud experienced was a dramatic upsurge in financial fraud from scandals triggered by distributed denial of service (DDOS) attacks such as Trojan, malicious software to enormous ATM withdrawals, POS payment and online fund transfer produced by organized fraudsters."* (Bank B: Interview, 2017).

> *"Yes, e-banking fraud experienced was phishing attacks which targeted bank customers' personal computers through virus, convince e-mails as legitimate online banking interfaces that deceived customers to submit their personal financial data."* (Bank C: Interview, 2017).

"Yes, most of the fraud incidents experienced were linked to electronic banking which included internet banking frauds, automated teller machines (ATMs) frauds and debit and credit card frauds, as well as identity frauds." (Bank D: Interview, 2017).

"Yes, in corporate banking, most of the frauds observed are associated with siphoning and electronic diversion of funds, even though fraudulent credentials and identity thefts were mostly the paths for frauds in Nigerian banks." (Bank E: Interview, 2017).

"Yes, the common fraud risks experienced which are still currently highest concerns in Nigerian banks today are internet banking frauds, automated teller machine [ATM] frauds, and identity frauds." (Bank F: Interview, 2017).

"This is my 18th year in the banking service, there is no how we would no record at least two significant fraud incidents from our branch offices, the common one I could recall are e-cheque transfer, impersonation of account, fund withdrawn from an ATM by unknown person, web base frauds, mobile banking frauds through and internet banking frauds through injecting of commands, vishing and smishing." (Bank G: Interview, 2017).

"Yes, the frauds experienced are internet frauds, ATM frauds, identity theft through phishing email, fraudulent transfers or transactions using stolen debit/credit card data, token, PINsentry cards, theft passwords and secret code Smartcard reader manipulation." (Bank H: Interview, 2017).

"Yes, e-banking frauds observed could be linked to e-cheque transaction frauds, card frauds and web transfer frauds." (Bank I: Interview, 2017).

"Yes, e-banking frauds experienced could be described as account impersonation, internet frauds, cheque cloning frauds, automated teller machine frauds and insider frauds (Bank staff)." (Bank J: Interview, 2017).

Table 6.4 Analysis of the Nature of E-Banking Fraud

Sub-Themes	Significant issues (Codes)	Interviewee by Bank
ATM and Card Frauds	Loss and theft of bank cards, identity theft, theft of passwords and secret code,	A, B, D, F, G, H, J, C, E
	improper disposal of damaged banking computer systems and customers' devices	
Frequency		9 (90%)
Mobile and Telephone Frauds	Injecting of commands, vishing and smishing, identity theft,	A, G
	hidden code, theft of passwords, secret code and loss of phone devices	
	theft of passwords and secret code, smartcard reader manipulation	
Frequency		2 (20%)
Debit/Credit Card Frauds	Token and PINsentry card theft, identity theft, loss and theft of bank cards,	D, H, I, G
Frequency		4 (40%)
Internet Banking Frauds	Identity theft, phishing, malicious software, pharming	A, B, C, D, E, F, G, H, I, J
Frequency		10 (100%)

Source: Thematic Analysis (2017)

Obviously, banking system fraud has existed for centuries, with the earliest acknowledged frauds relating to insider frauds, accounting manipulation, irregularity of accounts, overvalued assets and others (Beard, & Wen, 2007). Recently, frauds in the banking industry have become more sophisticated and cultured and have moved on to technologically based systems presented to customers. The Nigerian banking system too is undergoing this menace due to an upsurge in fraud occurrences, with 90% of the interviewees stating that fraud has increased over the last three years (Table 6.4). Most of the interviewees specified that they have witnessed diverse types of e-banking fraud incidences in a Nigerian deposit money bank in the last three years.

The interviewees were asked to remember and discuss a current fraud incidence that was distinctive. Almost all of the interviewees' comments on the nature and characteristics of fraud showed that most e-banking frauds are committed by identity theft, loss and theft of bank cards, injecting of commands, vishing and smishing, hidden code, theft of passwords, secret code and loss of phone devices, token and PINsentry card theft, identity

theft, loss and theft of bank cards, theft of passwords and secret code, smartcard reader manipulation, identity theft, phishing, malicious software and pharming, and improper disposal of damaged banking computer systems and customers' e-banking devices.

However, the development of technology in producing new services, together with the great growth in electronic banking, has permanently changed the business platform and how financial institutions perform their operations and minimize risks. As the banking sector increasingly relies on information technology, it is not amazing to discover that electronic fraud continues to rise in frequency, sophistication and volume.

This involves identity theft, vishing or phishing, ATM skimming, Trojans, pharming, phishing and mismanagement of debit and credit cards. In addition, when requested to identify the three leading types of frauds that were causing restlessness to both bankers and customers, it was not surprising that the responses of the participants in both qualitative and quantitative analyses referred to internet banking fraud, ATM fund transfer fraud and debit/credit card frauds as major categories of e-banking fraud in Nigeria. This is obviously in compliance with the global trend of the types of e-banking frauds that are most prevalent in the world.

Furthermore, from the survey research, the types of e-banking fraud that are paramount and frequently experienced by the Nigerian banking sector include internet banking fraud, ATM fund, transfer fraud and debit/credit card fraud. The strategies used include stealing and shoulder surfing of bank cards and customers' personally identifiable information such as name, date of birth, address, name of the bank and other bank-account-related information such as account number, account type, password, secret codes, memorable words and card long number.

The results of the survey research also indicated that customers' personally identifiable and bank account information could be sourced not only by stealing from the banks or individual customers but also through loss of cards and negligent disposal of banks' and customers' account portable electronic and non-electronic properties, for example bank

account documents, computer systems and other hardware storage devices such as phone sets, flash drives, external hard drives, CD discs, token cards and PINsentry cards.

In addition, this constitutes a real threat to banking sectors as fraudsters have direct access to banking systems and customers' financial records, personal information and finance through injecting commands, skimming devices, pharming, phishing, vishing and smishing and malicious software. According to the survey, despite the involvement of bank staff, the leading strategies of e-banking fraud involve identity theft. Therefore, in research to acknowledge and discover sophisticated prevention and detection mechanisms that will remove or reduce the opportunities for fraudsters to engage in such activities, there is need to examine the impacts of e-banking frauds, which are discussed in the next section as a second theme.

6.3.2 Factors Contributing to the Increase in E-Banking Fraud

Contributing factors to the increase in e-banking fraud were examined among ten senior staff of the selected Nigerian banks through this semi-structured interview question: "In your own opinion, what are the contributing factors to the rise in e-banking fraud?" The aim was to answer research question two: "What are the perceived factors that have considerable influence on the increase of e-banking fraud in Nigeria?". Here are the responses, followed by the analysis, findings and discussion.

> *"The modern technologies employed by banking systems make them more and more susceptible to several risks, particularly e-banking, such as card skimming, identity theft, phishing, SMSishing, vishing, viruses and Trojans, social engineering, spyware and adware, cyber stalking and website cloning, also wrong attitude of Nigerian police and fraud investigation bodies such as Economic and Financial Crimes Commission (EFCC) and Independent Corrupt Practices Commission (ICPC) towards investigating of crimes and banks also are not reporting fraud incident suspected to them."* (Bank A: Interview, 2017).

"Lack of oversight by senior management or line managers on nonconformities from existing procedures, business operation pressures to meet unreasoning targets, lack of technological mechanisms to recognize probable red flags, conspiracy between insiders and outsiders, and lack of adequate security at point of transaction through ATM, POS." (Bank B: Interview, 2017).

"Lack of customer and staff awareness, difficult to integrate data from diverse sources, weak litigation support in prosecution process, inadequate fraud detection tools and technologies." (Bank C: Interview, 2017).

"Economic situation, wrong value system, insider collusion, business pressure to meet targets, lack of customer awareness or enlightenment and ineffective prevention and detective technical mechanisms, including lawless habit of Nigerians and the enterprises." (Bank D: Interview, 2017).

"Higher level of illiteracy and lack of customer awareness, business pressure on bank staff and individual/personal pressure, ineffective antivirus and computer system software, and competent personnel for fraud investigation and detection such as professional forensic accountants, forensic financial analystss are not available to be employed in the bank, many of them preferred working with public sector." (Bank E: Interview, 2017).

"Diversities of factors are thought to have contributed to the upsurge in electronic banking fraud, but it has been driven by advanced technologies with fraudsters using social engineering scams such as vishing, phishing in amalgamation with more sophisticated internet and electronic attacks for instance infecting computer systems with malware [malicious software]." (Bank F: Interview, 2017).

"The prevalence of e-banking fraud risks is attributed to the inefficient internal controls, weakening ethical values, legal incompliance systems, lack of adequate due diligence of staffs and customers and lack of sophisticated preventive and detective technological tools because of insufficient fund for the investigation and detection." (Bank G: Interview, 2017).

"There are many factors contribute to the increase of e-banking frauds in Nigerian banks, such as ineffective skilled resources to manage data analysis, inadequate awareness of using forensic data analytics, lack of proactive and effective e-banking fraud risk monitoring, perceived excessive cost of software installation and management, and irregular electric power supply." (Bank H: Interview, 2017).

"Major challenges confronted by Nigerian banks in mitigating and preventing fraud are the lack of customer and employee awareness of fraud and its impacts; integration of information from various banking systems, inadequate resources and inadequate fraud detection tools, Nigerian security officers and other anti-fraud agencies are not competent enough or not bother for investigating online frauds in the community." (Bank I: Interview, 2017).

"Increasing risks of fraud emanating from adoption of innovative technologies which expose financial institutions as well as customers to the risk of hijacking of mobile phones, bank spoofing, SIM card cloning, stealing of the computer systems and included lack of customer awareness." (Bank J: Interview, 2017).

Table 6.5: Survey of Factors Contributing to E-Banking Fraud

Sub-Themes	Significant issues	Interviewees
Operational factors	Difficulty investigating crimes across borders, Issuing of counterfeit bank cards.	A, B, I, C and D
	Collusion between employees and outsiders, Difficulty integrating from various sources.	
	Changing of business strategies without changes in business procedures.	
Frequency		5 (50%)
Managerial Factors	Lost cards and stolen personal identification data, 'Inefficient internal controls.	B, D, E, C, I and G
	Pressure to meet business and personal targets, Improper disposal of portable devices.	
	Spending a long time on social media, Poor system administration and maintenance.	
	Lack of oversight by senior management on deviations from existing procedure.	
Frequency		6 (60%)
Educational Factors	Introduction of new products without adequate control and training in place.	D, E, H and I
	Customers and staff unawareness of fraud incidence, Inadequate computer knowledge and experience.	
	Use of the same password for different accounts, 'Incompetence of Anti-Crime Security Personnel.	
Frequency		4 (40%)
Technological Factors	Presence of phishing, identity theft, card skimming, vishing, viruses, deployment of keystroke loggers.	A, I, F, B, D, G and H
	Presence of Trojans, spyware and adware, website cloning and cyber stalking.	
	Lack of sophisticated antivirus software and weak passwords, Ineffective encryption backdoors.	
	Lack of fraud prevention and detection technological mechanisms,Lack of effective and efficient internet network.	
Frequency		7 (70%)
Legal Factors	Weak litigation support in prosecution process, Poor coordination with law enforcement.	D, C, I, G and A
	Incompliance with the law enforcement agency, Ineffective rule of law.	
	Lack of fraud risk assessment framework within the organization.	
Frequency		5 (50%)
Infrastructural and	Irregular electricity power supply in Nigeria, Insufficient financial resources.	I, C, B, E, G and H
Financial Factors	Lack of dedicated technology tools for investigation, 'Lack of effective and efficient internet facilities.	
Frequency		6 (60%)
Personnel Factors	Lack of forensic accounting professionals., 'Absence of quality forensic analysts.	E, H, I and A
	Lack of competent internal auditors, Lack of competent fraud investigators, 'Ineffective law enforcement agency.	
Frequency		4 (40%)

Table 6.4 explains that e-banking fraud generally tends to be perpetrated due to the existence of three main factors: rationalization, opportunity and financial pressure, in line with the fraud triangle. But there are also other factors, as can be seen from the survey. The respondents have characterized and attributed the upsurge in e-banking fraud to seven factors: operational factors, managerial factors, educational factors, technological factors, legal factors and infrastructural and financial factors.

Operational factors were demonstrated as the predominant operational risks for Nigerian banks today. These strongly hinge on the nature of administration and staff, and on the other hand, are influenced by corporate culture, working processes and the organizational structure of the institution. According to the survey results, 50% of the respondents among the staff agreed that the factors that contribute to the increase of e-banking frauds in Nigeria include difficulty investigating crimes across borders, issuing of counterfeit bank cards, collusion between employees and outsiders, difficulty integrating from various sources, changing of business strategies without changes in business procedures and inefficient internal controls, weakening ethical values, incompliance systems and lack of adequate due diligence of staff and customers (Banks A, B, I, C and D).

Moreover, difficulties in detecting fraud related to challenges in accessing and obtaining data about the fraud, particularly from across borders; data were also not received on a timely basis to facilitate and enhance detection of e-banking frauds (Bank A and Bank I). It is difficult to follow up and discover fraud in the absence of vital data, which may be held by other departments within and outside the country as e-banking fraud is a distance fraud. Challenges in detecting and investigating e-banking fraud brought different responses from the survey respondents. One of the difficulties faced by the banking institutions is that the fact that the staff are unenthusiastic and unwilling to incriminate their colleagues who are involved in perpetrating fraud; this frustrates and affects investigations (Bank B).

The banks also are facing great challenges due to lack of collaboration among bank management, law enforcement agencies and other financial and non-financial organizations (Banks A, D and I). Delays in investigating and prosecuting frauds occur

not only because of insufficient funds for investigation and prosecution but also due to the ineffectiveness and incompetence of law enforcement agencies and other anti-crime bodies such as police, the Economic and Financial Crimes Commission (EFCC) and the Independent Corrupt Practices Commission (ICPC). This has greatly contributed to the increase in fraud in the banking sector and in society generally (Banks A, D and I).

Furthermore, some fraud incidents recalled by the survey respondents or interviewees included deceitful withdrawals of funds from customers' e-bank accounts with the support of bank staff who leaked customers' and banks' electronic financial information to the fraudsters. Some bank staff encourage the increase in fraud by their lack of skill and negligence in performing their duties. For instance, some bank staff abandon their computer systems, leaving the customers to check their account information by themselves (Banks A, B, C and D).

It is not only that, the interviewees indicated the efficacy of tightening screening measures while recruiting fresh staff. This means that failure to follow due process and lack of effective employee background checks give opportunity to fraud penetration. Therefore, the main themes that developed from these responses involved the pervasiveness of collusion between employees and outsiders, changing of business strategies without changes in business procedures and inefficient internal controls, weakening ethical values, incompliant systems and lack of adequate due diligence among staff and customers (Banks A, B, C, D and I).

However, it is extremely difficult to detect a fraud perpetrated by the collusion of insiders and outsiders, because insiders are conversant with the bank and really involved in organizational control of the system. They may even be part of the organization's fraud investigation teams; instead of using their knowledge and position to safeguard the organization, these staff use it to commit fraud against the bank. Hence, to fight against fraud and to overcome collusion of insiders with outsiders in perpetrating fraud, there is a need for the establishment of effective internal controls which encourage staff rotation and segregation of duties, standard educational systems and fraud awareness schemes. These are discussed extensively in the next section.

The second category was managerial factors, which involved wrong attitudes among bank managements and customers toward the performance of their duties and safeguarding or managing e-banking systems. This includes lost cards and stolen personal identification data, pressure to meet business and personal targets, spending a long time on social media and mobile apps, saving e-banking passwords and other e-banking personal information in online diaries, lack of oversight by senior management on deviations from existing procedure, poor system administration and maintenance culture, lack of consistent monitoring of malpractice among employees, and improper disposal of e-banking portable devices and other damaged computer systems of the banks and customers (Banks B, D, E, C, I and G).

In addition, pressure to meet business and personal targets seems to be the major motivator for perpetrating frauds. The interviewees indicated that peer pressure, financial pressure, business pressure, opportunity and greediness are the motivators that encourage the occurrence of e-banking frauds (Banks B and E). The survey respondents further explained that the factors that influence the increase in e-banking fraud are associated with weak management systems and lack of effective supervision.

The third category is educational factors, which comprise the introduction of new products without adequate control and training in place, customer and staff unawareness of fraud incidence, use of the same password for different accounts, incompetence of anti-crime security personnel and inadequate computer knowledge and experience (Banks D, E, H and I). The fourth group is technological factors, which have to do with the presence of phishing, identity theft, card skimming, vishing, viruses, deployment of keystroke loggers, Trojans, spyware and adware, website cloning, cyber stalking, lack of sophisticated antivirus software and weak passwords; lack of fraud prevention and detection technological mechanisms; ineffective encryption backdoors; and ineffective and inefficient internet network (Banks A, I, F, B, D, G and H). The fifth group are legal factors; these encompass weak litigation support in the prosecution process, poor acquiescence with organizational policy, ineffective rule of law, lack of fraud risk

assessment framework within the organization, and incompliance with corporate governance and law enforcement agencies (Banks D, C, I, G and A).

Furthermore, the interviewees believed that the legal provisions available to banks for prevention and detection of fraud were feeble; there was no adequate fraud prosecution; legal and law enforcement were inadequate, including prosecutorial knowledge; and the legal procedure was inadequate, extremely difficult and prolonged (Banks D, C and I). Some respondents said that many fraud cases in courts remain unresolved for several years. In the process of these delayed cases some witnesses die or relocate abroad with material evidence, material information is lost, some lose interest in the issue and some fraud perpetrators are given opportunities to bribe their way out. Therefore, these factors affect the deterrence and mitigation power of fraud prosecution, greatly impairing banks' development (Banks D, C, I, G and A).

Obviously, the rampant bribery and corruption in the judicial system, which involves judges, prosecutors and police, has led to a massively increased acquittal rate among fraud perpetrators. Despite the challenges emanated by the legal or judicial system, the legal charges sometimes do not compensate for the money and time lost. The financial institutions do not find it advantageous to take legal or judicial action when the charges of prosecution are higher than the amount recuperated from the fraud.

Also, the interviewee from Bank B indicated that external fraud investigators such as police and other related bodies do not always persevere enough in the investigation due to a lack of skill, incompetence and lack of full understanding of the fraud cases under investigation. This is because the nature of their profession is not really based on investigation of financial fraud and cybercrime.

Also, there is inadequate compliance and collaboration with the internal investigation teams which are trained, well-educated and constantly practise as financial crime investigators in the banking system. Therefore, the judicial system needs to be reinforced and strengthened to minimize the occurrence of fraud in society. Collaboration and synergy should be enhanced and made effective among the investigation teams, which

comprise banks, the central bank, police, other external law enforcement agencies and anti-financial crime bodies.

Infrastructural and financial factors form the sixth set of factors. These were comprised of irregular electricity power supply in Nigeria, lack of dedicated technology tools for investigation and insufficient financial resources. Apparently, lack of effective equipment, lack of expertise, inadequate knowledge of information technology, and other related factors such as the absence of forensic laboratories, documents and online examiners are further challenges (Banks I, C, B, E, G and H). The detection and prevention of e-banking fraud is a costly issue: banks need to weigh and measure the cost of fighting against fraud with the reimbursements that would be recouped from doing so. The costs of fraud detection and prevention to banks could be assessed by the balance between cost or charge and benefit. The degree of organization commitment to fighting fraud is determined by the amount of financial resources available and budgeted for fraud detection and prevention. Therefore, very few of the interviewees had clear information on their banks' financial plans (budgets) for fraud detection and prevention: "In my bank, there are financial plans for skill development, investigation and information sharing for fraud prevention and detection, but they are not enough" (Bank B). The interviewees' specific explanation and defence for inadequate financial plans and ineffective fraud budgets was the sporadic nature of fraud occurrence; the existence of fraud is an unpleasant event.

The seventh factor is personnel factors: lack of forensic accounting professionals, lack of competent internal auditors, absence of quality forensic analysts, lack of competent fraud investigators and ineffective law enforcement agents.

6.3.3 E-Banking Fraud Prevention Mechanisms

Research question three, "What are the significant current prevention mechanisms for e-banking fraud in Nigerian banks?" was answered through this interview question: "What preventive mechanisms does your bank employ against e-banking fraud and how effective are the preventive mechanisms in your bank?" In the semi-structured interviews,

ten senior staff of the selected Nigerian banks were asked about this and related issues. Here are the responses followed by the analysis, findings and discussion.

> *"Frauds have been prevented through the internal audit and internal control but currently, the era of electronic transaction whistle-blower hotlines, data analytics (DA) and information technology (IT) mechanisms, security code, token cards, MasterCard SecureCode and smart card authentication have played major roles in e-banking fraud detection and prevention in Nigerian banks."* (Bank A: Interview, 2017)

> *"Several frauds have been prevented through the application of bank verification number (BVN) which came along with know your customers (KYC) procedure, biometric process and application of single account number with fingerprint. In addition, many frauds were detected through whistle-blower hotlines policy and data analytics (DA) procedure." (Bank B: Interview, 2017)*

> *"Fraud incidents experienced and discovered in this bank were through the means of internal whistle-blower, customer awareness, data analysis, automated monitoring software and during account reconciliation." (Bank C: Interview, 2017)*

> *"Majority of fraud were prevented through one-time password, multi-layer passwords and memorable words, external and internal whistle-blower policy, ATM surveillance, system monitoring software, automated data analysis and use of bank verification number (BVN)."* (Bank D: Interview, 2017).

> *"Obviously, application of bank verification number (BVN), whistle-blower, customers' complaint and fraud risk assessment have been the common mechanisms of fraud detection in Nigerian banks; forensic data analytics, data leakage prevention (DLP) software, have emerged as key mechanisms to detect e-banking frauds."* (Bank E: Interview, 2017)

"Technology and analytics tools such as BVN, internal and external surveillance tools and teams including management strategies in term of audits, whistle-blowers policy and monitoring teams for fraud risk management among Nigerian financial institutions includes effective fraud control policy, regulation and corporate code of conduct seems to be moderate mechanisms of e-banking fraud prevention." (Bank F: Interview, 2017)

"These frauds were prevented through CCTV at point of transaction, webcam, internal surveillance equipment, ATM monitoring surveillance, and through bank security officer and internal monitoring teams." (Bank G: Interview, 2017)

"As I said earlier, before the introduction of banking verification number (BVN), majority of frauds were prevented through customer screening and employees background check, whistle-blowers, customers' awareness, training and seminars, ATM monitoring surveillance, and some were reported by bank security officers and police." (Bank H: Interview, 2017).

"Well, in Nigerian banks today, particularly my bank here, bank verification number (BVN) is most effective mechanisms for both e-banking fraud prevention. There are other internet software and other applications for bank card fraud prevention such as passwords, memorable words, security code, token cards and smart card authentication included ATM monitoring surveillance system." (Bank I: Interview, 2017)

"Basic anti-fraud mechanisms we are using in my bank now which really effective in preventing e-banking frauds are bank verification number (BVN), biometric or finger print on our automatic teller machines, card transaction online monitoring software. Whistle-blowers and consumer education are also important means of preventing fraud, including internal and external auditors and internal control." (Bank J: Interview, 2017).

Table 6.6: E-Banking Fraud Preventive Mechanisms

Sub-Themes		Interviewees
Scientific Mechanisms	Bank verification number	A, B, C, D, E,
	Dedicated forensic technological tools for investigation.	F, G, H, I and J
	Use of security code, token cards, Mastercard SecureCode and smart card authentication.	
	Use of one-time password, multi-layer passwords and memorable words.	
	Use of PII, registered phone number, biometrics and data encryption.	
	Availability of closed circuit television (CCTV) security system.	
Frequency		10 (100%)
Legal and Synergies Mechanisms	Effective fraud control policy, regulation, corporate code of conduct, prosecution.	C, D, F, G, J
	Availability of effective whistle-blower hotline policy.	
	Collaboration with government, regulator, law enforcement agency and academia.	
Frequency		5 (50%)
Awareness and Education Mechanisms	Timely access to information by management, Effective fraud awareness training and seminars.	C, D, E, F, H, J
	Adequate consumer education on fraud prevention, 'personal accounting information protection.	
Frequency		6 (60%)
Surveillance Mechanisms	Use of cctv at point of transaction, Notified by law enforcement agency.	D, F, G, H, J
	Internal surveillance equipment,' ATM monitoring surveillance.	
		5 (50%)
Internal Control Mechanisms	Customer screening and employee background checks, 'Fraud internal control structure	A, D, B, C, E, F, J
	Automated address verification service (AVS) and automated phone call.	
	Intelligence gathering mechanisms, Risk and compliance programmes.	
	Clearly defined reporting structure and effective governance.	
Frequency		6 (70%)

Formerly, financial institutions focused on application of basic controls and processes to advance operational effectiveness, efficiency, oversight and control. Nowadays, however, there is an additional need to implement sophisticated mechanisms that are precisely aimed at preventing the menace of e-banking fraud, and empowering detection of fraud

incidents at an early stage. According to the responses from the survey respondents (see Table 6.6), the current mechanisms that have been applied by individual banks were grouped into five sub-themes: scientific mechanisms, awareness and education mechanisms, internal control mechanisms, legal and synergies mechanisms, and surveillance mechanisms.

Scientific Mechanisms constitute one of the best ways to prevent e-banking fraud from occurrence. All the respondents supported the view that e-banking frauds have been drastically reduced through the introduction of bank verification number (BVN), forensic technological tools for investigation, secret code, token cards, MasterCard SecureCode, smart card authentication, one-time passwords, multi-layer passwords and memorable words, registered phone numbers, biometrics, data encryption, and closed circuit television (CCTV) security systems (Banks A, B, C, D, E, F, G, H, I and J).

The interviewees were asked what current preventive mechanisms their banks had employed to prevent e-banking fraud. Most of the interviewees reflected positively on this question by saying that the most effective current preventive mechanism Nigerian banks employed was the bank verification number (BVN). These respondents testified that bank verification number (BVN) is part of biometric and customers' background verification processes, which developed in the form of a single number account.

Banks A, D, E and F concurred that, BVN has been the best preventive mechanism in Nigeria, it has affected all kinds of financial frauds, particularly identity frauds and accounting impersonation. Since its introduction, several financial frauds have been detected and many customers have been protected from the menace of the fraudsters. In short, it has reduced the financial frauds in the Nigerian banking sector.

Besides this, another scientific preventive mechanism used by the banks to protect their systems against e-banking fraudsters is to employ computer technology and protective software. The most common protective mechanisms used by banks are firewalls, secret code, token cards, MasterCard SecureCode, smart card authentication, one-time passwords, multi-layer passwords and memorable words, registered phone numbers,

biometrics, data encryption to block access to vulnerable devices and forensic technological tools for investigation and detection.

Awareness and education mechanisms are another set of mechanisms for e-banking fraud mitigation. Of the interviewees, 60% agreed if all the stakeholders have adequate knowledge of the causes, impact, prevention and detection of fraud through timely access to information by management, organizational learning for fraud prevention, adequate consumer education on fraud prevention and personal accounting information protection included effective fraud awareness training and seminars, this would minimize the incidence of fraud (Banks, C, D, E, F, H and J). Financial institutions have also used customer education and training on how to guard against fraud and how to protect their accounts. For instance, banks have been encouraged by the central bank to establish seminars and training for their customers and to use handbills, leaflets, magazines, media systems and customer care desks for the prevention and detection of frauds.

Internal Control Mechanisms form another way of preventing fraud from occurring. A total of 70% of the interviewees opined that customer screening and employee background checks, automated address verification service (AVS) and automated phone calls, fraud internal control structures, intelligence gathering systems and clearly defined reporting structures, effective governance, and risk and compliance programmes highly contributed to the reduction of e-banking fraud in the Nigerian economy (Banks A, D, B, C, E, F and J).

The segregation or separation of duties and roles was quoted as being an important mechanism of internal control. One of the interviewees (Bank D) explained how his bank suffered from loan fraud because of a lack of clear segregation of duties. The same staff member made an application for a loan, performed credit and background checks and offered the benefits fraudulently to himself. Hence, lack of separation of roles and duties leaves room for fraud in the organization. Therefore, there is a need for effective separation of roles and duties for proper and effective internal controls for fraud prevention and detection. Likewise, staff rotation and reassignment of duties, roles and responsibilities also enhance the prevention and detection of fraud in an organization.

Legal and Synergies Mechanisms call for compliance with law and organization policy and mitigating fraud through joint effort with other organizations. According to 50% of the respondents, e-banking fraud incidents were reduced by effective fraud control policies, regulation, corporate codes of conduct, prosecution, availability of effective whistle-blower hotline policy, collaboration with the government regulator, law enforcement agencies and academics (Banks C, D, F, G and J). Most of the respondents affirmed that their banks have a written corporate code of conduct and organizational policy to prevent unethical behaviour among the stakeholders, and that the banks give zero tolerance to unethical behaviour.

The interviewees believed there is not enough cooperation among the banks in sharing of information, which has been creating a problem in preventing and detecting frauds. Therefore, to have effective prevention and detection of perpetrated fraud there must be a cordial relationship among the banks, and policies and procedures for sharing fraud incidences and methods of preventing and detecting frauds. There should be forums and conferences where fraud incidences and methods of controlling them are discussed among the banks. There is the Nigeria Inter-Bank Settlement System (NIBSS), which performs a similar duty in Nigeria. NIBSS company has contributed immensely to the prevention and detection of e-banking fraud in Nigeria banking industry as a whole (Bank F). Furthermore, in the effective prevention of fraud through system technology, people are more important, as there are effective structures and policy statements when the right personnel are in place.

6.3.4: E-Banking Fraud Detection Mechanisms

Research question five, “What are the significant current fraud detection mechanisms for the e-banking frauds detection in Nigerian banks?” was answered through this interview question: “How are the fraud incidents that involved your bank typically detected?” In the semi-structured interviews, ten senior staff of the selected Nigerian banks were asked

about this perception and related issues. Here are the responses followed by the analysis, findings and discussion.

> *"Frauds have been detected through the internal audit and internal control but currently, the era of electronic transaction whistle-blower hotlines, data analytics (DA) and information technology (IT) mechanisms have played major roles in e-banking fraud detection and prevention in Nigerian banks."* (Bank A: Interview, 2017)

> *"Several frauds, both e-banking and non-e-banking frauds, have been detected and prevented through the application of bank verification number (BVN), which came along with know your customers (KYC) procedure, biometric process and application of single account number with fingerprint. In addition, many frauds were detected through whistle-blower hotlines and data analytics (DA) procedure."* (Bank B: Interview, 2017)

> *"Fraud incidents experienced and discovered in this bank were through the means of customer complaint or internal whistle-blower, data analysis, automated monitoring software and during account reconciliation."* (Bank C: Interview, 2017)

> *"Majority of frauds detected were exposed by customers' complaint, external and internal whistle-blower, and system monitoring software, automated data analysis and use of bank verification number (BVN)."* (Bank D: Interview, 2017)

> *"Obviously, application of bank verification number (BVN), whistle-blower, customers' complaint and fraud risk assessment have been the common mechanisms of fraud detection in Nigeria banks, forensic data analytics, data leakage prevention (DLP) software, have emerged as key mechanisms to detect e-banking frauds."* (Bank E: Interview, 2017)

> *"Technology and analytics tools such as BVN, internal and external surveillance tools and teams including management strategies in term of audits, whistle-*

blowers policy and monitoring teams for fraud risk management among Nigerian financial institutions seem to be moderate mechanisms of e-banking fraud detection and prevention." (Bank F: Interview, 2017)

"Some of these frauds were discovered through CCTV at point of transaction, webcam, internal surveillance equipment, ATM monitoring surveillance and through bank security officer and internal monitoring teams." (Bank G: Interview, 2017)

"As I said earlier, before the introduction of banking verification number (BVN), majority of frauds were detected through customers' complaints, internal and external, whistle-blowers, anonymous complaints, personal confession, ATM monitoring surveillance, and some were reported by bank security officers and police." (Bank H: Interview, 2017).

"Well, in Nigerian banks today, particularly my bank here, bank verification number (BVN) is most effective mechanism for both e-banking fraud prevention and detection. There are other internet software and other applications for bank card fraud detection and prevention." (Bank I: Interview, 2017).

"Basic anti-fraud mechanisms we are using in my bank now which really effective in preventing and detecting e-banking frauds are bank verification number (BVN), biometric or fingerprint on our automatic teller machines, card transaction online monitoring software. Whistle-blowers and anonymous complaints are also important means of detecting fraud including internal and external auditors." (Bank J: Interview, 2017).

Table 6.7 Theme: E-Banking Fraud Detection Mechanisms

Sub-Themes		Interviewees
Technical Mechanisms	Implementation of banking verification number (BVN) approach.	A, B, C, D, E, F, G, H, I
	Application of automated data analysis and intrusion detection system (IDS).	
	Use of transaction monitoring software., 'Application of internet banking fraud detection and data mining.	
	Application of forensic computer software and fraud risk assessments and investigations system.	
	Application of credit card fraud detection tools (Hidden Markov, Parallel Granular and Neural Networks).	
Frequency		10 (100%)
Monitoring Mechanisms	Fraud detection and monitoring team, 'Fraud controls, monitoring and analysis team.	C, D, F, G, J
	Monitoring the internet to detect and close malware websites.	
Frequency		5 (50%)
Complain and whistle-blow	Customers' complaints, 'Internal and external whistle-blowers.,Anonymous complaints.	A, C, D, E, F, G, H, J
	Personal Confession., 'Customers' complaints.	
Frequency		8 (80%)
Surveillance Mechanisms	Use of CCTV at point of transaction,'Internal surveillance equipment.	D, F, G, H, J
	ATM monitoring surveillance, 'Notified by law enforcement agency.	
Frequency		5 (50%)
Management Protocol	Internal and external audits, 'Management review, 'Online accounting reconciliation.	A, B, C, E, F, J
Frequency		6 (60%)

As stated in Table 6.7 above. Technical Mechanisms: 100% of the survey respondents reported that some frauds had been discovered through the means of the banking verification number (BVN) approach, automated data analysis, intrusion detection systems (IDS), transaction monitoring software, internet banking fraud detection and data mining, forensic computer software, fraud risk assessment and investigations systems and credit card fraud detection tools (Hidden Markov, Dynamic Key Generation and Group Key, and Parallel Granular and Neural Networks).

Monitoring mechanisms: 50% of the respondents consented that monitoring mechanisms are major techniques for detecting e-banking frauds in Nigeria; they include fraud detection and monitoring systems, monitoring the internet to detect and close malware websites, fraud controls, and monitoring and analysis teams.

Stakeholders' complaints and Whistle-Blowers Mechanisms: 80% of the survey respondents revealed that many frauds have been detected through customers' complaints, internal and external whistle-blowers, anonymous complaints and personal confessions (Banks A, C, D, E, F, G, H and J).

The interviewees also indicated that whistle-blowers have played significant roles in fraud detection. One interviewee (Bank H) related an incident where a whistle-blower from outside the bank came and alerted the bank about an illegal withdrawal from an ATM in the bank premises. There are other mechanisms of fraud detection, such as recruitment of new employees and staff rotation. Many frauds have also been discovered through customer complaints and personal confessions. The respondents confirmed that some of the e-banking frauds that have been discovered were through customers complaining when they discovered fraudulent withdrawals from their accounts.

Surveillance mechanisms: 50% of the respondents reported that some frauds, particularly at ATM points, had been detected through CCTV at the point of transaction, internal surveillance equipment, ATM monitoring surveillance and bank security officers and police (Banks D, F, G, H and J). Internal and external surveillance equipment also play significant roles in fraud detection. As stated by Bank G, through CCTV, "someone was caught with mask at ATM who made cash withdrawal with another person's bank card in 2015."

Management protocol, 60% of the respondents explained that some e-banking frauds had been detected during online accounting reconciliation, management review, and internal and external audit assessments.

6.4 Proposed Model of E-Banking Fraud Prevention and Detection

The findings of quantitative and qualitative show that technological mechanisms, fraud monitoring and internal controls, customer complaints and whistle-blowing, surveillance mechanisms, staff- customer awareness and education, legal and judicial controls, and institutional and organizational synergy mechanisms would have considerable influence

on prevention and detection of e-banking fraud in the Nigerian banking industry. Therefore, these mechanisms were used to form a tentative model shown below in Figure 6.4, which is titled "Seven-Star of E-Banking Fraud Prevention and Detection".

Figure 6.1: Seven-Star of E-Banking Banking Fraud Prevention and Detection

Moreover, the findings revealed that technological mechanisms play a significant role in e-banking fraud prevention and detection. However, this was in contradiction to the level of importance given to the issue of e-banking fraud. Only a few Nigerian banks have

acquired dedicated and sophisticated technological prevention and detection mechanisms and recruited experts such as forensic accountants, chartered fraud investigators, qualified auditors and other related anti-crime agencies. Instead, the banks are investigating e-banking frauds through ad-hoc staff from the management team, who is selected when fraud incidents occur.

Financial resources for fraud prevention and detection constitute another significant issue. According to the findings, most of the banks had no precise financial budget for fraud prevention and detection, while some respondents expressed their views that the financial budget for managing and controlling fraud could not be a separate item but could be recognized as the fund spent on staff training, procurement and implementation technology, human resources, internal controls and employment of security officers.

The effectiveness and success of e-fraud detection and prevention could be determined by the methodologies and mechanisms employed by the banking industries and how frauds are detected. The findings from the qualitative research revealed that almost all the e-banking frauds that had been detected were discovered through the banking verification number (BVN), whistle-blowers, internal surveillance systems, customers' complaints, and fraud detection and monitoring teams. The degree of consistency of the effectiveness of these methods shows that these are useful and efficacious approaches to fraud prevention and detection.

However, although these mechanisms of prevention and detection conformed to and were consistent with the expectations of the institutions, they are not consistent with the nature of e-fraud – "electronic fraud, fraud at a distant place and time" – which requires dynamic laws and sophisticated technological advancements. Thus, to have effective prevention and detection of e-banking fraud in Nigerian banking institutions, there is a need for the institutions to invest in sophisticated technological prevention and detection tools such as monitoring the internet to detect and close malware websites, monitoring phishing-related websites and software, fraud controls, monitoring and analysis software, automated data analysis and transaction monitoring software.

In addition, the response to the incidence of fraud in the Nigerian banking sector is another significant issue, as the quantitative and qualitative evidence revealed that the prosecution of the fraud perpetrators was an approach rarely pursued by the banks' management. Simple expulsion or dismissal was the only action taken by banks against suspected fraudsters; this could work for internal fraudsters, but what about external fraudsters? There is a seeming lack of institutional involvement, such as synergy amongst banking institutions, police, the judiciary and other financial anti-crime agencies. This has already been illustrated in the qualitative findings, where an interviewee said that Nigerian police officers lack the required skill and capacity for e-banking fraud investigation, and that the prosecution of e-banking fraud incidents is uncertain, expensive and lengthy. The interviewee further linked this to failings in the legal and judicial system. There is no obvious definition and clarification within the law about certain fraud types such as bank card fraud, telephony fraud and web fraud; this has been problematic for prosecuting e-banking frauds.

Above all, the respondents explained that the cost of criminal or civil prosecution, amalgamated with inappropriate legal systems, have been impediments for the banks in effectively prosecuting egregious e-banking frauds. Likewise, the respondents indicated that the non - prosecution of fraud had been a business decision on the part of the banks. A lot of fraud incidences were not followed up to the stage of prosecution by the banks so as to protect their successful reputations.

Internal control is another significant issue. Nigerian banks have been found wanting in registration of potential customers and aspects of recruitment and selection of bank employees. As elucidated throughout this research, e-banking fraud is committed by an entity, a group of individuals. It is essential, therefore, that the banking institutions employ the right people as staff and register accounts for the right customers.

Therefore, inadequate and improper background verifications during recruitment of staff and opening accounts for potential customers give huge and ample opportunities to external and potential internal fraudsters in the banking industry. As for availability of information, even the present "Certificate of Good Conduct" from the Nigerian police is

rarely reliable as the data can be possibly altered and manipulated. Hence, there is no specific data base either for the employee or individual citizen reference checks in Nigeria, which makes it more difficult for banking systems to secure essential information from reliable sources. However, all blame cannot be placed solely on the database centre; bank managements also need to be included, as the study indicated that Nigerian banks have disregarded dependable references and employed staff with known fraud histories. Therefore, there is a need for bank management to exercise effective and sensible caution in selecting and recruiting employees and to recognize this as a significant mechanism for controlling and managing fraud in the country (see Table 6.8).

Table 6.8: Proposed E-Banking Fraud Prevention and Detection Mechanisms

Mechanisms	Prevention	Detection
Technological Mechanisms	Application of:	Dedicated Forensic Technological Tools
	Bank Verification Number,	for Investigation,
	Closed Circuit Television (CCTV) Security System	Implementation of Banking Verification
	Use of Token Cards, MasterCard, and Smart Card	Number (BVN) Approach.
	Biometrics and Data Encryption	Application of Automated Data Analysis
	Registered Phone Number	and Intrusion Detection System (IDS),
	Authentication: Use of Security Code,	Use of Transaction Monitoring Software,
	One-Time Password, Multi-Layer Passwords	Data Mining, 'Fraud Risk Assessments
	and Memorable Words	and Investigations System (FRIS) and
	Installation of Computer Antivirus Software	Application of Credit Card Fraud Detection
		Tools such as Hidden Markov, Parallel Granular
		and Neural Networks
Legal and Judicial Control	Effective Rule of Law, Fraud Control policy,	
Mechanisms	Regulation, Corporate Code of Conduct,	
	and Prosecution. 'Availability of Effective	
	Collaboration Whistle-Blower Hotline Policy,	
	with Government, Regulator, Law Enforcement	
	Agency and Academia	
Fraud Monitoring, Internal	Customer Screening and Employee Background Checks	Fraud Detection and Monitoring Teams,
Control and Administrative	Automated Address Verification Service (AVS)	Monitoring the Internet to Detect
Mechanisms	and Automated Phone Calls, Fraud Internal Control	and Close Malware Sites,Fraud Controls,
	Structure, Intelligence Gathering Mechanisms,	Monitoring and Analysis Teams,
	Clearly Defined Reporting Structure,	Internal and External Audits, and
	and Effective Governance,	Management Review Online
	Risk and Compliance Programmes	Accounting Reconciliation
Staff-Customer Awareness	Timely Access to Information by Management	
and Education Mechanisms	Adequate Consumer Education on Fraud Prevention	
	Effective Fraud Awareness Training and Seminars,	
	Staff Workshops on Customer Account Information	
	Protection	
Customer Complaints and	Whistle-Blowers Hotline Policy	Customers' complaints, Personal Confessions,
Whistle-Blowing Mechanisms		Internal and External Whistle-Blowers, and
		Anonymous Complaints.
Surveillance Mechanisms	Use of CCTV at Point of Transaction,	Detection Through CCTV at Point of Transaction,
	Internal Surveillance Equipment,	Internal Surveillance Equipment,
	ATM Monitoring Surveillance,	ATM Monitoring Surveillance,
	Law Enforcement Agency (Police), and	Notified by Law Enforcement Agency (Police),
	Company Security Officer.	and Company Security Officer.
Institutional/Organizational	Fighting Fraud in Collaboration with Other Financial	
Synergy Mechanisms	Institutions Within and Outside the Country, with	
	Other Home and Foreign Non-Banking Organizations,	
	such as Communication Organizations, Courts,	
	Law Enforcement Units, Anti-Crime Organizations	
	and Other Business Organizations.	

6.5 Integration of Findings with Theories and Literature Review

This section discusses how the findings of this study relate to the present theoretical contexts of criminological theory and management theory used in this study. The purpose of this was to evaluate how the theories have informed the study and how the findings have developed the existing theoretical frameworks. Both the quantitative and the qualitative findings have inferences and implications of the theories of frauds that have been acknowledged (routine activity theory and fraud management lifecycle theory). These theories were discussed extensively in Chapter 3 and were applied in this section. Particularly to answer research questions 2, 3 and 4 of the study.

6.5.1 Routine Activity Theory (RAT)

The routine activity theory has been extensively discussed in Section 3.1, but this section will focus on its application and relationship with the present findings on prevention and detection of e-banking fraud in Nigerian banks. The routine activity theory was introduced by Cohen and Felson (1979). It describes fraudulent activities through three important bases that meet in time and space in the sequence of daily events: motivated offender, suitable target and capable guardians. Routine activity theory holds that fraudulent activities will probably materialize when there is a combination of a suitable target and a motivated offender (fraudster) without the presence of a capable guardian in a conjunction of space and time (Miller, 2014). This answer research questions 2, 3 and 4 of this study:

1. What are the perceived factors that have considerable influence on the increase in e-banking fraud in Nigeria?
2. What are the current significant mechanisms for e-banking fraud prevention in Nigerian banks?
3. What are the current significant mechanisms for e-banking fraud detection in Nigerian banks?

6.5.1.1. Motivated Offender

Motivated offenders are individuals or groups of people who have not only had the capacity to perpetrate fraud but are also enthusiastic about doing so. In the context of this study, a good profile for differentiating the typical characteristics of the motivated offender (fraudster) is based on the types of e-banking fraud. Motivated offenders are those that are methodologically motivated through the opportunities that surround them and typically have a definite victimology connected. Therefore, the motivations are available opportunities to commit fraud. Benefits and risks that make a person or group of people become fraudsters or become involved in perpetrate frauds can also involve a perpetrator's intelligence, canniness and cleverness (Gottfredson & Hirschi, 1990).

Motivation is what is considered an appropriate temperament to perpetrate a fraud, or the physical influences which made it probable for a potential fraudster to become involved in perpetrating fraud. It exists when an individual or group of people belong or have access to the following elements which are deduced from the findings of the quantitative and qualitative surveys and are in line with the literature review in Chapter 2 of this study. They must be an insider who has access to customers' e-banking account information, other insiders, account passwords, sniffing, spoofing, Man-in-the-Middle, electronic banking devices, application software, denial of service, social engineering and virus software; this could motivate them to see opportunities to commit fraud. However, this study also extensively investigated the other two elements of the routine activity approach: suitable targets and capable guardians.

6.5.1.2 Suitable Targets

Suitable targets are individuals or objects or entities that are identified and targeted by offenders (fraudsters) as vulnerable entities. As discussed in Chapter 3, elements regarded as suitability have been grouped into two acronyms: "CRAVED" represents concealable, removable, available, valuable, enjoyable and disposable (Clarke, 1999) and "VIVA" means value, inertia, visibility and accessibility (Sutton, 2009). Sutton (2009) related the

two acronyms and established that they deal with distinguishable attributes, arguing that the elements of VIVA describe the characteristics that draw the attention of the fraudsters to the targeted entity or that make the targeted entity (banks and e-banking customers) suitable to be defrauded, while the CRAVED elements are related to characteristics that make the attractive object available for fraudsters (Anderson, 2006). Congruently, in the context of this study, suitability of the target refers to the factors contributing to the increase in e-banking fraud (Sections 5.4.1 and 6.3.2). The responses of the respondents showed that the factors contributing to the increase in e-banking fraud are the factors that make the targets (banks or individuals) attractive or suitable to be defrauded. These have been categorized into operational factors, managerial factors, educational factors, technological factors, legal factors and infrastructural and financial factors.

Furthermore, these operational factors – the factors that could make the targeted customers or banking institutions attractive to motivate fraudsters – emerged through the mode of banks' business operations and behaviour of banks' staff towards their business, which reflect several issues that are contributing to the increase in e-banking fraud in the Nigerian banking industry. These are the difficulty of investigating crimes across borders, availability of insiders and outsiders, difficulty integrating from various sources and lack of effective and efficient internet network facilities, changing of business strategies without changes in business procedures, and lack of fraud risk assessment frameworks within organizations. This corroborates the view of Kinkela and Harris (2014) that fraud involves the teaming up of bank staff with security agents in both national and international networking.

In the same vein, technological factors are the visible, available, disposable and accessible factors in both internal and external environments of the banking institutions which make the targeted entity or individual attractive to the perpetrators of fraud on the electronic system. These include as phishing, identity theft, card skimming, vishing, SMS phishing, viruses, deployment of keystroke loggers and Trojans, spyware and adware, website cloning and cyber stalking; lack of sophisticated antivirus software and weak passwords;

episodic electricity power supply; lack of prevention and detection techniques and tools; and ineffective encryption backdoor's (Sections 5.4.1.7 and 6.3.2).

This substantiates the arguments of Peotta et al. (2011), who adopted an attack tree model to represent the major attacks on e-banking and how they associate with each other, such as phishing attacks, social engineering, malware to gain control of system devices, and malware and fake web pages for credential theft from an authentic user. Omariba, Moses and Wanyembi, (2012) also classified the various factors that are contributing to electronic banking fraud, such as port scanners, social engineering attacks, phishing, Trojans, pharming, denial of service, PIN hacking, super user exploits and server bugs.

Legal and law enforcement processes are other attractions, suitable factors that make the target customers or banks vulnerable to fraud and contribute to the increase in e-banking fraud. These factors include weak litigation support in the prosecution process in court, poor coordination with law enforcement by banks and customers, and lack of rule of law in society (Sections 5.4.1.7 and 6.3.2). In addition, corruption in the law enforcement agencies such as courts and police in Nigeria contributes to inadequate prosecutions of fraudsters and investigation of frauds, which has impaired reliability and discouraged some banks from prosecuting those that perpetrate fraud because of fear of an unsuccessful outcome. Prosecution of suspected fraudsters is particularly difficult in a country where the regulators, police, lawyers and judges are vulnerable to bribes (Cule & Fulton, 2009). Therefore, potential fraudsters could see these as opportunities to commit fraud.

Similarly, educational factors could also boost the upsurge in e-banking fraud; these are factors that make customers vulnerable or give room for fraudsters to perpetrate fraud. In accordance with the findings, these include the introduction of new products without adequate controls and training in place, customer and staff unawareness of fraud incidence, use of the same password for different accounts, incompetence of anti-crime security personnel and inadequate computer knowledge and experience. In conjunction with the above, Choplin and Stark (2013) found that bank customers are vulnerable to electronic banking fraud because of lack of education and awareness.

Moreover, maintenance and management factors emanated from the negative habits of customers towards their bank account facilities, such as loss of bank cards, stolen personal identification data, spending a long time on social media; and from the ineffective performance of management, which can lead to pressure to meet business and personal targets, lack of oversight by senior management on deviations from existing procedure, and poor system administration and maintenance culture.

Personnel factors are the factors arise through unavailability of fraud investigation experts. These also contribute to the increase in e-banking fraud; for example, unavailability of forensic accounting professionals, lack of competent internal auditors, absence of quality forensic analysis, lack of competent fraud investigators and ineffective law enforcement agencies.

The findings from both the quantitative and qualitative research revealed that banks are vulnerable to fraud when there is a lack of facilities and inadequate resources such as episodic electricity power supply, lack of dedicated technological tools for investigation, lack of effective internet facilities and insufficient financial resources in the banks; these factors therefore contribute to the increase in e-banking fraud (Sections 5.4.1.7 and 6.3.2). Therefore, routine activity theory argues that e-banking target accessibility increases and contributes to e-banking fraud when there is an absence of capable guardianship; and e-banking target visibility is increased by the frequency and variety of e-banking routine activities, for instance e-payment, online money transfer, POS, direct debit, checking of the account balance at cybercafés and standing orders. This corroborates the opinion of Deloitte (2015), in the study "India Banking Fraud Survey", that there is an increase in e-banking fraud occurrence in the banking sector because of the lack of tools and technology to discover potential red flags.

However, in agreement with the fraud triangle concept of "opportunity" (Cressey, 1953), but not with the main theoretical framework of this study, Lister (2007) elucidated opportunity as the "fuel that keeps the fire going", which means that however high the degree of motivation, a fraud perpetrator cannot commit fraud without having the opportunity. Taylor (2011) supported this view with examples such as poor management

of turnover, improper segregation of duties and ineffectiveness of organizational structure.

In addition, Soltani (2014) agreed that position is an opportunity for someone that is a fraudster or trust violator to commit fraud. He also opined that there is a link between power to conceal fraud and opportunity to commit fraud. Wolfe and Hermanson (2004) described opportunity as a weakness in the internal controls of an organization which allows employees to commit fraud. Albrecht, Albrecht and Albrecht (2008), mentioned that the lack of an audit trail, ineffectiveness of internal controls, weakness of the board of directors, lack of effective anti-fraud disciplinary policy, and other factors serve as perceived opportunities to commit fraud.

6.5.1.3 Capable Guardian

A capable guardian is someone or something whose presence will prevent a probable fraud from happening; its absence makes it likely that fraud will be committed (Felson, 1995). A capable guardian comprises anyone within an environment or working as a guard of property, persons such as police and anti-crime agencies, and all other prevention and detection mechanisms that have been discussed in Sections 5.4.2,5.4.3,6.3.3 and 6.3.4.

Furthermore, as elucidated in the findings of this study, prevention and detection mechanisms are capable guardians for e-banking fraud. These were grouped into scientific mechanisms, awareness and education mechanisms, internal control mechanisms and legal and synergies mechanisms. These groups could be defined as passive physical guardianship (secure browsing, installation of antivirus software, and use of one computer system), active personal guardianship (changing of passwords and security), and avoidance, personal guardianship (avoiding staying online for a long time, avoiding transferring money online, avoiding online purchasing and purchasing through credit or debit card).

Scientific mechanisms are the technological strategies and tools applied to prevent and control e-banking and cyber frauds in the banking industry. Scientific mechanisms are among the best ways to prevent e-banking fraud from occurring. Both qualitative and quantitative respondents reported that e-banking frauds have been drastically reduced through the introduction of the bank verification number. This is supported by the Central Bank of Nigeria, which through the Bankers' Committee and in cooperation with all other banks introduced the Nigeria Inter-Bank Settlement System (NIBSS).

As stated in Chapter 2, the bank verification number was introduced due to growing incidents of compromise of conservative security systems (PIN and password) and an increased demand for sophisticated security for sensitive information in the Nigerian banking system. The aim of the bank verification number was to protect banks' customers from identity theft and other financial frauds emanating from the Nigerian banking industry (Orji, 2014).

Moreover, there are other scientific mechanisms used in Nigerian banks, such as forensic technological tools for investigation, secret code, token cards, MasterCard SecureCode, smart card authentication, one-time passwords, multi-layer passwords and memorable words, registered phone numbers, biometrics, data encryption, and closed-circuit television (CCTV) security systems. This is substantiated by the survey of Chan et al. (1999), who concluded that electronic banking fraud prevention and control focused on fraud prevention software, smart card authentication, one-time passwords and biometric authentication. Phua et al. (2010) further testified that biometric technology provides a better authentication technique and improves security.

The survey respondents reported that surveillance mechanisms have played a significant role in detecting and discovering e-banking frauds in Nigerian banks. Respondents testified that some frauds, particularly at ATM points, had been detected through CCTV at the point of transaction, internal surveillance equipment, ATM monitoring surveillance and bank security officers and the police. Internal and external surveillance equipment also play significant roles in fraud detection. The respondents also declared that some e-

banking frauds were detected during online accounting reconciliation, management review, and internal and external audit assessments (Sections 5.4.3.4, 6.3.4).

Awareness and education mechanisms form another set of methods for e-banking fraud mitigation. The qualitative and quantitative respondents agreed that if all the stakeholders have adequate knowledge of the causes of fraud and the impacts and consequences of committing fraud through timely access to information by management; organizational learning for fraud prevention; and adequate consumer education on fraud prevention and personal accounting information protection, including effective fraud awareness training and seminars, this would minimize the incidence of fraud. Appropriate educating and training of employees and proper awareness among customers of misconceptions connected with frauds are significant for the deterrence and discovery of fraud (Sections 5.4.2.4, 6.3.3).

However, financial institutions have also used customer education and training on how to guard against fraud and how to protect their accounts. For instance, an interviewee reported that banks have been encouraged by the central bank to establish seminars and training for their customers and to use handbills, leaflets, magazines, media systems and customer care desks for the prevention and detection of frauds.

Internal control mechanisms are another way of preventing fraud from occurring. Interviewees opined that customer screening and employee background checks, automated address verification services and automated phone calls, fraud internal control structures, intelligence gathering systems and clearly defined reporting structures, effective governance, and risk and compliance programmes greatly contributed to the reduction of e-banking fraud on the Nigerian economy.

Legal and synergies mechanisms also serve as capable guardians. This call for compliance with law and organization policy and mitigating fraud through the joint effort of the law enforcement forces and other concerned organizations. Survey respondents agreed that e-banking fraud incidence was reduced by effective fraud control policies, regulation, effective corporate codes of conduct, prosecution, availability of effective whistle-blower

hotline policies, and collaboration with government regulators, law enforcement agencies and academics (Sections 5.4.2.4, 6.3.3). Most of the respondents affirmed that their banks have a written corporate code of conduct and organization policy to prevent unethical behaviour among the stakeholders and that their banks give zero tolerance to unethical behaviour.

The survey respondents believed that there is not enough cooperation among the banks in the sharing of information, which has created a problem in preventing and detecting fraud. Therefore, to have effective prevention of fraud and detection of perpetrating fraud, there must be a cordial relationship between the banks, and policies and procedures for sharing fraud incidences and methods of preventing and detecting frauds. There should be forums and conferences where fraud incidences and methods of controlling them can be discussed among the banks. As reported by an interviewee in the fieldwork, there is the Nigeria Inter-Bank Settlement System, which performs a similar duty in Nigerian. This company has contributed immensely to the prevention and detection of e-banking fraud in Nigeria. Furthermore, in the effective prevention of fraud through system technology, people are more important as there will be effective structures and policy statements when the right personnel are in place.

Consequently, in the context of e-banking fraud, capable guardianship can be reflexive physical guardianship; for example, operating only one electronic system, using antivirus, email spam filtering, safekeeping of credit/debit cards, token card, PINsentry and secured browsing. It can be active personal guardianship through the changing of passwords, security settings, memorable words, PIN codes and secret questions (Wilcox et al., 2007). It can also mean avoidance personal guardianship by reducing time spent on the internet, for example, when online purchasing and online banking, and logging out of one's email box and electronic banking on time when finishing. If these online activities are well guarded, motivated electronic fraudsters may be deterred from suitable e-banking targets to perpetrate electronic banking frauds.

Correspondingly, the Parliamentary Joint Committee (2004) on the Australian Crime Commission's investigation of cybercrime (2004) observed that a suggestion by the

Association of Australian Bankers emphasized customers' responsibility for personal protection or self-safety from fraud rather than the banking industry's responsibility for protecting the security of their customers. Therefore, while financial institutions will habitually recompense sufferers for their monetary losses, they are unwilling to take the issue any further. Lynch (2005) contended that there is no monetary incentive for the banking industry to prevent electronic fraud. However, recently banks have made improvements in security using two-factor and three-factor identifications, whereby customers are required to use multiple techniques, such as a digital token and password (Smith 2007).

The present study tested the application of the routine activity approach and the policy hypothesis that the adoption of passive physical guardianship, active personal guardianship and avoidance guardianship will help in combating e-banking fraud. The findings show that the application of the routine activity approach reduces e-banking fraud.

6.5.2 Fraud Management Lifecycle Theory

The fraud management lifecycle is the proactive use of prevention, deterrence, investigation, policy, analysis, detection, mitigation and prosecution of fraudsters (Wilhelm, 2004). The fraud management lifecycle theory is a network lifecycle where each node or stage in the lifecycle is a combined entity that is a form of interrelated and interdependent actions, operations and functions (Albrecht et al., 2009). The provisions of this theory with its components were adopted in the examination of electronic banking fraud prevention and detection in Nigerian banks. The adoption of this theory resulted from its methodical approach to combating fraud. In the first place, this theory creates an environment that deters people from perpetrating both online and offline frauds; it embraces the strategies to prevent frauds from happening; and even if there is occurrence of fraud, it has provision for a purposeful detection strategy, reprimand and punishment

of the criminals. Therefore, the theory was adopted to answer research questions 3 and 4 of this study.

1. What are the current significant mechanisms for e-banking fraud prevention in Nigerian banks?
2. What are the current significant detection mechanisms for e-banking fraud detection in Nigerian banks?

6.5.2.1: Deterrence

Deterrence is accomplished through creating fear of difficulty and consequences of perpetration, to discourage or turn aside would-be fraudsters from attempting fraudulent activity (Kimani, 2013). Deterrence is characterized by activities and actions targeted at preventing and stopping fraud before it is attempted by making the effort to perpetrate fraud dreadful, unattractive or life-attacking (Ibor, 2016). Therefore, from the perspective of this study, in the qualitative and quantitative findings deterrence is considered by functions, actions, operations and activities envisioned to prevent fraud before it occurs; specifically, to discourage the attempt at committing fraud. The respondents agreed that deterrence mechanisms include policy implementation, implementation of laws and regulations, card activation, internet passwords, card pin codes, anti-fraud portals, biometric identification systems, electronic passport verification portals, bank verification number (BVN), a single point of connection to all bank schemes, data management programs and legal and reputational fraud management. Therefore, deterrence should include establishing authentication measures and appropriate authorization privileges; physical and logical access maintenance; authentication control processes; customer verification; satisfactory infrastructure security to control appropriate restrictions and boundaries for both external and internal users, data and activities; and integrity of transactions, information and records

6.5.2.2: Prevention

Prevention is the second component of the fraud management lifecycle; it comprises functions to avert fraud from happening (Wilhelm, 2004). Prevention includes activities

and actions to stop fraud from occurring (Ibor, 2016). It should be supreme in any e-banking fraud control system. E-banking fraud prevention is the actions and activities to reduce opportunities for e-banking fraud to happen, such as the bank verification number (BVN). It must be centred on a fraud assessment development that reflects a bank's vulnerability to fraudulent activities, within an integrated e-banking approach (Vasiu & Vasiu, 2004).

The qualitative and quantitative findings show that fraud prevention in electronic banking will only be effective if all the following are implemented: introduction of bank verification number (BVN), forensic technological tools for investigation, secret code, token cards, MasterCard SecureCode, smart card authentication, one-time passwords, multi-layer passwords and memorable words, registered phone numbers, biometrics, data encryption, and closed circuit television (CCTV) security systems. If all the stakeholders have adequate knowledge of the causes, impact, prevention and detection of fraud through timely access to information by management, organizational learning for fraud prevention, adequate consumer education on fraud prevention, and personal accounting information protection including effective fraud awareness training and seminars, this would minimize the incidents of fraud.

Customer screening and employee background checks, automated address verification services (AVS) and automated phone calls, fraud internal control structures, intelligence gathering systems and clearly defined reporting structures, effective governance, and risk and compliance programmes all greatly contributed to reducing e-banking fraud on the Nigerian economy. So, did fraud control policy, regulation, corporate codes of conduct, prosecution, availability of effective whistle-blower hotline policies, and collaboration with government regulators, law enforcement agencies and academics.

The interviewees believed there is not enough cooperation among the banks in sharing of information, which has been created a problem in preventing and detecting fraud. Therefore, to have effective prevention of fraud and detection of perpetrating fraud, there must be a cordial relationship between the banks, and policies and procedures for sharing fraud incidences and methods of preventing and detecting frauds. There should be forums

and conferences where fraud incidences and methods of controlling fraud can be discussed among the banks such as NIBSS. NIBSS has contributed immensely to the prevention and detection of e-banking fraud in Nigeria (Bank F). Furthermore, in the effective prevention of fraud through system technology, people are more important, as there will be effective structures and policy statements when the right personnel are in place.

6.5.2.3 Detection

Detection is the third stage; it is made up of activities and actions to reveal or uncover the presence of or attempts at fraud, such as statistical monitoring programs that are used to locate and identify fraud subsequent, during and prior to the completion of the fraud perpetration (Wilhelm, 2004).

In the quantitative and qualitative research, respondents reported and suggested that effective detection of e-banking fraud could be achieved when the following mechanisms are implemented: the bank verification number approach; automated data analysis; intrusion detection systems (IDS); transaction monitoring software; internet banking fraud detection and data mining; forensic computer software; fraud risk assessments and investigations systems; and credit card fraud detection tools such as Hidden Markov, Dynamic Key Generation and Group Key and Parallel Granular and Neural Networks. All these are highly effective tools of fraud detection (see Table 6.1).

Furthermore, survey respondents agreed that monitoring mechanisms are major techniques for detecting e-banking frauds in Nigeria: fraud detection and monitoring systems, monitoring the internet to detect and close malware websites, fraud controls, and monitoring and analysis teams.

Interview respondents revealed that many frauds have been detected through customers' complaints, internal and external whistle-blowers, anonymous complaints and personal confessions. There are also other mechanisms of fraud detection, such as recruitment of

new employees and staff rotation. The respondents confirmed that some e-banking frauds have been discovered through customers complaining when they discovered fraudulent withdrawals from their accounts. Therefore, developing a principle or policy that motivates stakeholders who recognize fraudulent incidences to report this to the appropriate quarter through an ethical channel or hotline should be a priority for banks.

Survey respondents reported that surveillance mechanisms have played a significant role in detecting and discovering e-banking frauds in Nigerian banks. Respondents testified that some frauds have been detected, particularly at ATM points, through CCTV at the point of transaction, internal surveillance equipment, ATM monitoring surveillance, and bank security officers and the police. Internal and external surveillance equipment also play significant roles in fraud detection. Respondents also declared that some e-banking frauds had been detected during online accounting reconciliation, management review, and internal and external audit assessments.

6.5.2.4 Mitigation

The aim of the mitigation component is to discontinue fraudsters' fraudulent activities or to hinder fraud perpetrators from completing or continuing to perpetrate fraud (European Central Bank, 2013). The findings of the qualitative and quantitative surveys show that e-banking fraud could be mitigated by deactivating banking cards (credit or debit cards), barring an account passcode or PIN, blocking an account, message authentication, one-time passwords (OTPs), personal identification numbers, biometric characteristics, payment authentication codes to be sent to customers, customer awareness, customer verification and account origination. In the following stage, known as "analysis", losses that happened regardless of deterrence, detection, and prevention components are known and measured to control the causes of the damage by using statistical methods.

6.5.2.5 Policy

Policy is the sixth stage of the fraud management lifecycle theory; it deals with the creation, evaluation, communication, and deployment of policies to minimize the occurrence of fraud. Holling and Clark (1983) demonstrate the significance of policy development and organizational control in the prevention of fraud and fraudulent activities in an organization. This theory suggests four key areas of policy improvement that are indispensable in preventing fraud: full understanding of fraudsters' behaviour, dissemination of useful information on organizational policy, broadcasting sanctions, and the implementation and enforcement of sanctions (Wilhelm, 2004). In this study, the respondents consented that e-banking fraud was reduced by implementing effective fraud control policies, regulation, corporate governance, corporate codes of conduct, prosecution, availability of effective whistle-blower hotline policies, and collaboration with government regulators, law enforcement agencies and academics. Most of the respondents affirmed that their banks had a written corporate code of conduct and organizational policy to prevent unethical behaviour among the stakeholders, and that the banks give zero tolerance to unethical behaviour. Furthermore, in the effective prevention of fraud through system technology, people are more important as there will be effective structures and policy statements when the right personnel are in place.

6.5.2.6 Investigation

The investigation stage involves having sufficient information and enough evidence to end fraudulent incidents, recover stolen assets and produce evidence that will support the prosecution and conviction of the fraud perpetrators (Wilhelm, 2004; Albrecht et al., 2009). Fraud investigations are concentrated upon three main aspects of activity: investigation of law enforcement harmonization, internal investigations and external investigations.

The interviewees in this study believed that there is not enough cooperation among the banks in sharing of information, which has created a problem in investigating e-banking fraud. Therefore, to have effective prevention of fraud and detection of perpetrated fraud there must be a cordial relationship among the banks and policymakers, and procedures for sharing fraud incidences and methods of preventing and detecting frauds. There should be forums and conferences where fraud incidences and methods of controlling fraud can be discussed among the banks. There is the Nigeria Inter-Bank Settlement System (NIBSS), which performs a similar duty in Nigeria. This company has contributed immensely to prevention and detection of e-banking fraud in Nigeria (Bank F).

Similarly, quantitative respondents indicated that external fraud investigators such as police and other related bodies do not always persevere enough during investigation due to lack of skill, incompetence and lack of full understanding of the fraud cases under investigation. This is because the nature of their profession is not really based on financial fraud and cybercrime investigation, and results from inadequate compliance and collaboration with the internal investigation teams who are trained, well-educated and constantly practise as financial crime investigators in the banking system.

Therefore, the judicial system needs to be reinforced and strengthened to minimize the occurrence of fraud in society. Collaboration and synergy should be enhanced and made more effective among the investigation teams, which comprise banks, the central bank, police, other external law enforcement agencies and anti-financial crime bodies. Routine and rigorous investigations are required for an effective relationship with law enforcement to enhance deterrence of fraud. Electronic surveillance is one of the methods used in this stage of investigation.

Wilhelm (2004) also recommends that the prevention and detection of fraud requires a complete fraud management lifecycle and effective connectivity of its components, which encompass deterrence, detection, prevention, analysis, mitigation, investigation, policy and prosecution. This means that effective management and control of fraud needs a balancing of the complementary and competing components of the fraud management lifecycle in financial institutions. Failure to effectively balance the components of this

fraud management lifecycle and to adopt appropriate techniques that will ensure perfect integration of its components may result to poor control and management of fraud in financial institutions.

Therefore, the fraud management lifecycle can be said to be the fraud management network. Each of its components represents a node and the lifecycle represents the network, which is seen as a group of entities that is made up of interdependent and interrelated functions, operations and actions (Wilhelm, 2014). These platforms of the fraud management lifecycle must be carefully and successfully incorporated and balanced to exploit the advantages or merits of developments in fraud detection and prevention technologies, to protect the Nigerian economy from shortages of valuable resources, and to protect the Nigerian banking sector from fraudulent activities.

6.5.2.7 Analysis

As said earlier, analysis is recognised as the activities to understand and identify losses that happened regardless of the detection, deterrent, mitigation and prevention of e-banking fraud. Analysis must be performed to examine the effects of the fraud management stages of activities on banks and victim customers. The cost of fraud incidences must be assessed and properly estimated to ascertain exert prioritization of fraud cases. The analysis component collects data concerning performance from other components of the fraud management lifecycle and feedback the outcomes of the performance of each of the components. The analysis gives the performance reporting matrices that permit fraud management to provide calculated, relevant, informed decisions. The procedures of analysis involve examination of causes and the volume of shortages or losses, the reporting and examination of investigation and performance analysis, reporting and evaluation of aggregate and individual detection (rule) performance, the examination and feedback on e-banking fraud prevention and detection, analysis of the impact of the aggregate or individual stages of the fraud management on the increase factors, prevention and detection mechanisms of e-banking fraud.

However, the findings have disclosed that policies and prosecutions have not been effectively handled to prevent and detect banking fraud in Nigeria due to the rampant bribery and corruption in the judicial system. This, which involves judges, prosecutors and police, has led to a massively increased rate of fraud perpetrators being acquitted. Therefore, information technology and legal resources are significant keys to the effectiveness of e-banking activities as well as the effectiveness of the whole fraud management units in the banking industry.

Conversely, the underlying statement is that unawareness of the fraud management lifecycle and, subsequently, the need to integrate and balance the technological improvements and activities available to each component, results to inefficient and ineffective fraud management. Therefore, without this understanding and awareness, fraud management experts in the banking industry are unlikely to communicate successfully with each other, with their colleagues in other institutions, and within their individual banking businesses.

6.5.2.8 Prosecution

As discussed earlier, prosecution focuses on the judicial and prosecutorial system of authority along with law enforcement. The main objectives of prosecution in the arena of fraud is to discipline and castigate the fraudsters with the aims of preventing further theft; establishing, maintaining and enhancing the banking sector's reputation; and deterring fraud incidences. Prosecution is the conclusion of both positive and negative outcomes of the fraud management lifecycle stages. Outcomes are negative if the fraud was successfully committed and positive if the fraud was detected, and the fraudster was identified, arrested, detained and charged. This stage also includes criminal restitution, asset recovery, and conviction with its attendant deterrent value.

Overall, the findings indicate that the activities of each stage of the fraud management lifecycle theory, and their interdependence and consanguinity, have a collective and considerable influence on combating e-banking fraud. Therefore, the present study contributes to the importance of the fraud management lifecycle theory because it has

been shown to serve as a theoretical framework to examine e-banking fraud prevention and detection in the Nigerian banking industry. As the first study of its nature in the Nigerian context, this thesis assists in the critical analysis of interrelationship of the eight components of the fraud management lifecycle for the prevention and detection of fraud. These components of fraud management lifecycle: prevention, deterrence, investigation, policy, analysis, detection, mitigation and prosecution are based on the debate about whether individual perpetrators can be dissuaded from perpetrating fraud.

Moreover, the interviewees and questionnaire respondents have confirmed the presence of the fraud management lifecycle components in the Nigerian banking industry, while showing that the activities of fraud detection and prevention in the industry have yet to be balanced with all the components of the fraud management lifecycle. The findings indicate that technological and legal environmental factors intensely influenced the ability of the banking sector to perform activities in some of the fraud management lifecycle components.

For example, one of the interview respondents indicated that detection and prevention mechanisms were difficult to implement due to the nature of the law and technology required. When fraud management experts in the banking industry fail to balance the different components of the fraud management lifecycle effectively and fail to integrate innovative technologies into each component of the lifecycle, it exposes the banks into fraud losses and the benefits of improvements in fraud detection and prevention technologies are subsumed and muted. Therefore, there is a need for innovative technology, effective awareness and efficient legal practices for mitigating e-banking fraud in the Nigerian banking industry.

6.6: Summary

This chapter has dealt with the qualitative research with the use of content and thematic analyses. It has elucidated the major findings that arose from the interviews conducted with executives from the selected Nigerian banks. The major themes of the qualitative survey were in line with the theoretical framework and the research objectives. These were the nature of e-banking frauds, contributing factors of e-banking frauds, prevention mechanisms of e-banking frauds and detection mechanisms of e-banking frauds.

The nature of e-banking frauds was sub-themed into automated teller machine (ATM) frauds, mobile frauds, telephone banking frauds, debit/credit card frauds and internet banking frauds. Contributing factors for e-banking frauds involve operational factors, managerial factors, educational factors, technological factors, legal factors, personnel factors, infrastructural and financial factors. Preventive mechanisms of e-banking frauds include scientific mechanisms, legal and synergies mechanisms, awareness and education mechanisms, surveillance mechanisms and internal control mechanisms. Precisely, prevention and detection mechanisms of e-banking frauds comprise technical mechanisms, monitoring mechanisms, complaints and whistle-blowers mechanisms, surveillance mechanisms and management protocol (see Table 6.9 and Figure 6.1).

Moreover, the findings of the quantitative and qualitative research analyses have some significant implications based on their relationship with the literature and their consistency with the theoretical framework. The interpersonal and structural relationships between banking institutions play a vital role in determining the incidence of e-banking fraud and its detection and prevention. However, the synergy of the anti-fraud agencies, such as the EFCC, police, court and intra-bank organizations such as the Nigeria Inter-Bank Settlement System (NIBSS) are not being effectively used to detect and prevent e-banking fraud. Also, failure, breach of trust and incompetence on the part of legal institutions and law enforcement agencies have, in the sight of the banking industry, made it tremendously problematic to prosecute fraud perpetrated within and across borders in a cost-effective and timely manner.

Electronically, e-banking fraud prevention and detection have suffered from menaces such as unavailability of funding resources and lack of sophisticated technology and forensic prevention and detection mechanisms. In conclusion, there are advanced developments and transformations in technology that could enhance effective prevention and detection of e-banking fraud. Banks need to invest extensively in technological.

CHAPTER SEVEN: CONCLUSIONS AND RECOMMENDATIONS

7.0 Introduction

The objective of this study was to provide a contribution to the knowledge and understanding of fraud in the Nigerian banking industry. The research that has been performed within this research study was comprehensive and wide-ranging, and addressed a broad variety of fraud-related subjects in Nigerian banking institutions. However, this study only reproduces a fractional view of fraud in the Nigerian banking industry, only examining the e-banking fraud prevention and detection in the Nigerian banking sector.

There is a profound bedrock of historical, political and social issues that are excluded from the scope of this study, which has engaged only within the e-banking service aspect of nature, contributing factors, challenges, prevention and detection. In view of this, the information discussed in this study provides a significant foundation for discussion of the strategies and mechanisms for preventing and detecting distinct types of e-banking fraud in the banking system and other financial institutions within Nigeria. Thus, this chapter elucidates the practical and theoretical contribution made by this study, summarizing the major findings in respect of the research questions; explaining the implications for knowledge, theory, the judiciary and policymakers; revealing policy implications and providing recommendations. Finally, this chapter will conclude with an explanation of limitations to the study and discussion of areas for upcoming research.

7.1 Summary of Major Findings and Conclusions

The emphasis of the discussion was based on these research questions:

1. What are the e-banking fraud risks that are of high concern in the Nigerian banking sector?
2. What are the perceived factors that have considerable influence on the increase in e-banking fraud in Nigeria?
3. What are the current significant mechanisms for the e-banking fraud prevention in Nigerian banks?
4. What are the current significant mechanisms for e-banking fraud detection in Nigerian banks?

Each of these research questions was discussed from both primary and secondary researches generated from the findings of quantitative and qualitative analyses which were also supported by the literature reviewed.

Firstly, the opening research question discussed the nature of e-banking fraud in Nigerian banking institutions. This question was mainly answered by the quantitative survey which also supported by interview participants in qualitative analysis. The findings indicated that internet banking fraud, mobile banking fraud and Automated Teller Machine fraud are the current e-banking fraud risks that are of high concern in Nigerian banks.

Secondly, it is obvious that the banking institutions in Nigeria are aware of e-banking fraud that has become a major problem in the industry. The findings on question 2 indicated that ineffective banking operations and internal controls, improper banking management, lack of bank staff education and training, lack of sophisticated technological prevention and detection tools, lack of customer awareness, ineffective legislation and law enforcement, inadequate infrastructural and financial resources, economic pressure and presence of sophisticated technology in the hands of fraudsters have observed as the major reasons behind the rapid increase in e-banking fraud in Nigerian banking enterprises.

Thirdly, the last two research questions of this study addressed the challenges of how to mitigate the menace of fraud in the Nigerian banking industry. In the qualitative and quantitative research findings, e-banking fraud detection and prevention mechanisms have been shown to follow six approaches: technological, legal and synergy, awareness and education, surveillance, internal control and whistle-blowers mechanisms. Likewise, the empirical literature and theoretical review indicated that prosecution and dismissal of the fraudsters are the best mechanisms for preventing fraud this was also supported by both the quantitative and qualitative researches.

7.2 Implications of the Findings

The findings and analyses of this study have some significant implications; not only for academic researchers or scholars and accounting practitioners, but also for policymakers in the financial institutions and anti-fraud agencies in both the private and public sectors.

7.2.1 Implications for Theory

This study is the first study to examine e-banking fraud prevention and detection in the Nigerian banking industry. Although. previous studies have focused on banking frauds but were only on online banking fraud and credit card fraud prevention (Williams, 2016; Belan, Mane & Patani, 2014; Kathirvel, 2013). Even though several related studies have been conducted on online banking and credit card fraud in various parts of the world, particularly in the United Kingdom and United States of America, no broad studies like this current study has been done in an underdeveloped nation such as Nigeria. Peradventure, if any, related study has been conducted in Africa, it was only piecemeal. This is therefore the first study of this nature in the Nigerian context; thus, it has contributed to the theoretical literature and the growing body of knowledge on e-banking fraud prevention and detection and also, to the practices of effective e-banking industry.

In Chapter 3, the two theories were combined to discuss e-banking fraud prevention and detection. Firstly, the study identified the importance of routine activity theory in the prevention and detection of e-banking fraud. However, routine activity theory (RAT) commences from the principle of the presence of a motivated offender. It does not demarcate its connotations; consequently, it is incapable of demonstrating the basic methodologies of detecting fraud and of answering basic questions such as "Who are motivated offenders?", "What attributes do motivate offenders have?" and "Why some people more interested and (motivated) than others to perpetrate frauds? And also, what are the mechanisms of prevention and detection of fraud?" These questions have been answered by the current study.

Secondly, the findings, submit that the activities of each stage of fraud management lifecycle theory and their interdependence and consanguinity have a collective and considerable influence on combating e-banking fraud. The eight components of prevention, deterrence, investigation, policy, analysis, detection, mitigation and prosecution are based on the view that individual perpetrator can be dissuaded from perpetrating fraud.

However, the interview and questionnaire respondents confirmed that, at present in the Nigerian banking industry, the activities of fraud detection and prevention have yet to be balanced with all components of the fraud management lifecycle. The findings indicated that policy and legal, environmental factors intensely influenced the ability of the banking sector to perform activities in some of the fraud management lifecycle components.

For instance, the findings have disclosed that policy and prosecution have not been effectively handled to prevent and detect banking fraud in Nigeria due to the rampant bribery and corruption in the judicial system. This involves judges, prosecutors and police, and has led to a massively increased rate of fraud perpetrators being acquitted. Therefore, information policy and legal resources are significant keys to the effectiveness of e-banking activities as well as the effectiveness of all fraud management units in the banking industry.

Conversely, the underlying statement is that unawareness of the fraud management lifecycle and, subsequently, the need to integrate and balance the technological improvements and activities available to each of its components, results in inefficient and ineffective fraud management. Therefore, without this understanding and awareness, fraud management experts in the banking industry are unlikely to communicate successfully with each other, with their colleagues in other institutions, and within their individual banking businesses.

For example, one of the interview respondents indicated that detection and prevention mechanisms were difficult to implement due to the nature of the laws and technology required. When fraud management experts in the banking industry fail to balance the different components of the fraud management lifecycle effectively and fail to integrate innovative technologies into each component of the lifecycle, this exposes the banks into fraud losses and the benefits of improvements in fraud detection and prevention technologies are subsumed and muted. Therefore, there is a need for innovative technology, effective awareness and efficient legal practices for mitigating e-banking fraud in the Nigerian banking industry.

Also, as discussed earlier, prosecution focuses on the judicial and prosecutorial system of authority along with law enforcement. The main objectives of prosecution in the arena of fraud are to discipline and castigate the fraudsters with the aims of preventing further theft; establishing, maintaining and enhancing the banking sector's reputation; and deterring fraud incidences. The prosecution is the conclusion of both positive and negative outcomes of the fraud management lifecycle stages. Outcomes are negative if the fraud was successfully committed, and positive if the fraud was detected and a fraudster was identified, arrested, detained and charged. This stage is also comprised of criminal restitution, asset recovery, and conviction with its attendant deterrent value.

Lastly, the current study has added to the theories of fraud by providing a new model, titled the "Seven-Star Model" (see Figure 6.1), which includes seven prevention and detection mechanisms for e-banking fraud. These are technological mechanisms, fraud monitoring and internal controls, customer complaints and whistle-blowing, surveillance

mechanisms, staff-customer awareness and education, legal and judicial controls, and institutional and organizational synergy mechanisms. Therefore, this is a considerable contribution to the theory in the aspect of financial fraud prevention and detection.

7.2.2: Implications for the Judicial System

Due to the challenges emanated by the legal or judicial system, banks find that prosecutions sometimes do not provide compensation for the money and time lost. Nigerian banking institutions do not find it advantageous to take legal or judicial action when the charges of prosecution are higher than the amount recuperated from the fraud. The findings of this study have identified that there are feeble legal provisions for prevention and detection of fraud available to the Nigerian banking industry.

The respondents agreed that there were inadequate fraud prosecution procedures, ineffective legislation and law enforcement, inadequate prosecutorial knowledge and unproductive legal procedures in the Nigerian legal system. Some respondents also said that many fraud cases in the courts remained unresolved for several years; in the process of these delayed cases, some witnesses died or relocated abroad with material evidence, material information was lost, some lost interest in the issue some fraud perpetrators were given an opportunity to bribe their way out. Therefore, these factors affect the deterrence and mitigation power of fraud prosecution, greatly impairing banks' development. Thus, there is need to investigate the impact of the judicial system on the prevention and detective of financial fraud in Nigeria.

7.2.3: Implications for Policymakers

Obviously, this study has provided other significant contributions to knowledge of theories and empirical applications in the aspect of policymaking in banking institutions.

The study serves as a source of information on theoretical literature on e-banking fraud prevention and detection in the academic setting. In addition, it provides significant information for decision-makers in the banking sector to modify their practices for combating e-banking fraud and other related fraud types.

Moreover, the findings of this present study have resulted in substantial provisions for legal, regulatory and law enforcement institutions; policymakers within the executive and legislative arms of Nigerian government; executive directors of Nigerian financial institutions; and all professional accounting and banking bodies to be able to design better control and security systems against fraudulent practices within their operations.

7.3 Recommendations

The findings of this study have generated some recommendations for Nigerian banking institutions, as well as for the general transformation of the Nigerian legal and financial sectors to minimize the menace of e-banking fraud in the country.

In relation to policy, it is obvious that e-banking fraud prevention and detection mechanisms will work if the national government continues to assign significant funds and other resources to their improvement and advancement. The findings show that without extradition protocols, and inter-jurisdictional policy, e-banking fraud will not be combated or controlled.

Moreover, the findings of this study have revealed that improvement of the legal and jurisdictional system is a function of restructuring the judiciary and the law, through a combination of effective training for judges, attorneys and police on the causes, impacts, challenges, prevention and detection of e-banking fraud and other banking crimes. Therefore, advanced training is necessary for all police officers through an Anti-Crime Financial Training Programme in order to enable police units in the country to gain advanced knowledge and ability to aid in combating e-banking and other financial fraud.

This would enhance the effectiveness and efficiency of fraud control and mitigation within the industry.

Similarly, education has its own role to play. The Nigeria Inter-Bank Settlement System Plc (NIBSS) and the Nigeria Electronic Fraud Forum (NeFF) should educate prosecutors and police on the causes of e-banking fraud. Workshops and seminars should not only be for bank stakeholders, particularly customers and employees; they also should include police and the prosecutors of fraud cases. This could enhance legal skill and minimize the number of cases of fraud left undecided by the courts due to inadequate legal skills and insufficient evidence.

Also, it is obvious that the Nigerian legal system must be structurally rehabilitated towards e-banking fraud prevention and detection to advance the strength of the Nigerian banking industry. According to the findings of the study, there must be improvements in the court system in terms of the cost and time required for prosecuting fraud to influence the banks to use prosecution as a tool for deterring and mitigating fraud.

The issue of potential e-banking fraud is noted as one of the factors that put off both individuals and business organizations from the idea of internet banking. It affects the banking industry's reputation and reduces the acceptance of mobile banking even in an environment where it might feasibly be a development of the banking industry. According to the findings, potential fraud has a negative effect on investors' confidence, affecting the country's capacity to contend with other countries in relation to economic development and foreign direct investment (FDI). Therefore, for the Nigerian banking industry to minimize the level of fraud, there is a need for government intervention to mitigate the structural problems of law enforcement agencies and prosecutors to enhance and advance the banks' perception of the judicial system.

Furthermore, individual banks should pay attention to e-banking fraud because the research has revealed that fast implementation of e-banking services security has become significant as banks have introduced e-banking to all their customers. Implementation of sophisticated mechanisms for prevention and detection should be in place, particularly

for the top e-banking fraud types in Nigeria: ATM fraud, internet banking fraud, mobile banking fraud, and credit and debit card fraud.

E-banking fraudsters are unlikely to be caught by the current security systems within the individual banks. Therefore, the Nigerian banking systems need to create an external environment in the facet of external information technology structures, as these structures may be vulnerable to attack from the outside, which may result in momentous losses. Nigerian banking institutions, either jointly or individually, could check for best practice of preventing and detecting e-banking fraud in other banks or institutions worldwide.

Additionally, customer awareness crusades are another issue. Banking institutions are reluctant to involve themselves in customer awareness crusades about e-banking fraud, even though they are recognized to be active, because of the potential for reputation loss. Brand identity is vital to maintaining and sustaining customer loyalty to banks; therefore, the Nigeria Inter-Bank Settlement System Plc (NIBSS) and the Nigeria Electronic Fraud Forum (NeFF) should take on this significant role by providing education to customers and informative materials for all deposit money banks (DMBs) regarding the causes and impacts of e-banking fraud, including how to report, prevent and detect it. This might prominently improve attention to the early-warning scheme of customers' awareness without exposing the brand and product reputation of any bank to risk.

Furthermore, the establishment of a centralized fraud database would be very significant and would enhance the fraud investigation capacity of the fraud investigation teams of the deposit money banks.

Likewise, centralization of Nigerian residents' identities in a nationwide database system will have a positive impact on the e-banking fraud investigation scheme and in establishing a fraud management system in the Central Bank of Nigeria; it will also boost and strengthen jurisdictional prosecution of fraud. Therefore, this study recommends the establishing of a fraud database by the individual banks and a nationwide residents' identity database.

The Nigerian banking sector should provide antivirus software to all their customers by e-bank accounts; they should be given access to download and install it on their individual systems. This will protect individual e-banking customers from the fraudsters using viruses to hijack their account information.

The other recommendation is based on prevention and detection of e-banking fraud perpetrated by fraudsters from abroad. The Nigeria Inter-Bank Settlement System Plc (NIBSS) and the Nigeria Electronic Fraud Forum (NeFF) should associate with foreign banking associations. Such a relationship could enhance their capacities for prevention and detection of e-banking frauds from both within and outside the country and assist the cultivation of international methods and technical knowledge on preventing and detecting e-banking fraud for the use of the Nigerian banking industry.

In the same vein, it is obvious that almost all business and non-business organizations patronize the banking industry and engage with e-banking activities such as electronic points of sale (EPoS) and automated teller machines (ATMs). Therefore, Nigerian banks should create relationships, synergies or partnerships with government and non-government organizations, including other financial institutions within the nation, for sharing information and technology for prevention and detection of e-banking fraud, as well as improving knowledge and technology transfer. This would also provide an opportunity to educate all organizations that prevention and detection of e-banking fraud is not only a fight for a single organization but also involves the cooperation of all organizations within the region.

7.4 Limitations of the Study

This study has produced a comprehensive assessment of the prevention and detection of e-banking fraud in the Nigerian banking industry. Nevertheless, there are certain limitations that were noticed in consideration and discussion of the results of this study.

First, the outcomes of the study are geographically restricted. Although they produce an insight into the Nigerian banking industry and the structural condition of the political and judicial systems, they cannot be applied to other nations except as general lessons and findings. In other words, these results can be applied only to the Nigerian economy. In addition, the results are temporally limited, which means that some history and present conditions were described; that is, the results of the study are based only on the historical and present conditions of Nigerian industry. Therefore, the results may not be applicable to the conditions after changes have taken place to the current situations of government or banking technology.

Second, the sample size considered for this study was relatively small to capture the view of the entire Nigerian banking sector, although efforts were made to guarantee its representativeness. Furthermore, to attain representativeness, samples were drawn from deposit money banks (DMBs) in Nigeria. The researcher selected those staff in the selected banks that are highly knowledgeable and have enough experience of e-banking fraud; for example, fraud investigators, auditors, risk assessment managers, security managers and such like. Choosing respondents who directly head the responsibilities and functions of managing and controlling fraud may assist in reducing the restriction of representativeness. Hence, it could be perfect to accept that the views articulated by three or four respondents in the qualitative research could be adequate in representing the banks' intuitions, attitudes and views about e-banking fraud, as these participants were the professional experts and specialists in the banking systems.

The third limitation is respondent bias. There could be unintentional response bias from the respondents, resulting in some aspects of e-banking fraud not being noticed. As stated

above, there are some cases where respondents might have felt it would be risky to disclose or might not have really known the complete scope of the e-banking fraud incidences. Considering this and the importance of banks' brand reputation in retaining customers and investors, it is probable that some respondents might have withheld some information that could have altered the interpretation and understanding of the findings, or else that these respondents had no access to the required information in the initial stage. For instance, there may be limited information on exact fraud prevention and detection technologies or the scope and scale of fraudulent incidents within the banks.

Therefore, these issues might lead to respondent bias by hiding possibly vital information that could alter the results of the study if it were discovered. Although, to avoid this, the researcher cross-checked the information from both quantitative and qualitative sources and the respondents were assured that the information supplied would be confidential, this remains a significant issue within the outcome of the study. In this case, it is possible that biased results would produce an excessively optimistic and minimized view of e-banking fraud in Nigerian banking institutions, as the respondents would be unwilling to give the impression that e-banking fraud was more greatly prevalent than it basically is.

Hence, there is the possibility that this study is exaggeratedly optimistic in relation to the assessment rate of e-banking fraud occurrence, although it is not predictable that there is significant overassessment of the effectiveness of the e-banking fraud prevention and detection mechanisms or other related issues. Any such bias was not obviously detectable by the researcher as the responses from the participants proved consistent; nevertheless, it is best if the probability of bias is recognized rather than disregarded.

In addition, the study has created an issue concerning perceptions of the perpetrators' and respondents' motives. This research does not state what the perpetrators really think. Therefore, there is a possibility of bias due to the interest of fraud fighters in describing the causes and challenges of e-banking fraud.

Fourth, having access to the participants is a critical aspect of gathering data for research. Irrespective of the nature of fraud, it is a subtle and sensitive issue, not only in Nigeria

but also in the global economy. Some individual and organizational respondents tend to see the researcher as an invigilator, which leads them to treat researchers with suspicion. In some cases, participants withheld some information, claiming that they were limited by codes of confidentiality.

Due to this fact, some relevant questions pertinent to specific categories of e-banking fraud were excluded from the research. Gaining access was very hard, but through management and personal interaction connections with the respondents were achieved. Therefore, despite the challenges that accompanied gaining access to the respondents, the outcomes of this study can be used to make restricted generalization.

Fifth, one of the major limitations that this research encountered was the insufficient of theoretical frameworks to describe e-banking fraud in a nation where there is an inadequate infrastructural facility, lack of technology, mismanagement and an ineffective judiciary as the major contributors to e-banking fraud. There are also scanty literatures available regarding e-banking fraud within Nigeria and her environment. This, united with the limited information collected from the respondents and the existing theoretical framework, have made it difficult to extensively explore e-banking fraud.

7.5 Areas for Future Research

This study has produced enough information regarding Nigerian banking institutions and the prevention and detection of e-banking fraud within them. However, there are some aspects that need to be covered which could be exploited by future research. A few potential aspects of research and the approaches by which this research could be performed are acknowledged and discussed below.

One aspect of future research is e-banking fraud across borders. Most of the participants in the qualitative survey indicated that e-banking fraud across borders was a growing concern, and it was at the same time very difficult to investigate due to the challenges encountered with jurisdictional procedure, ineffective rule of law in Nigeria, and the

absence of synergy with other countries. An extensive study regarding e-banking fraud across borders could produce an understanding of the scope of this challenge and classify how it could possibly be resolved, or else provide a technique for mitigating the menace posed by the growth of cross-border e-banking fraud. Such a study might most effectually be conducted by means of technological and documentation research, looking at legislative and judicial records, documents from foreign agencies, records from banking systems and other aspects of the detection and prevention of cross-border e-banking fraud. This study would be large in scale and would require a considerable volume of documents from several organizations. In fact, if effectively conducted, such a study might not only be academically research but also legal research.

Another aspect of future research is customer awareness of e-banking fraud. The findings of this research indicate that a lot of e-banking frauds were detected through customers' complaints about something amiss observed in their e-banking accounts. Nevertheless, the Nigerian banking system has not given adequate attention to developing customer awareness for the deterrence of e-banking fraud due to banks not wishing to give customers the negative impression that they are vulnerable to e-banking fraud. However, with the belief that customer awareness will be an effective mechanism for preventing and detecting e-banking fraud, training and educating customers regarding preventing the occurrence of fraud and discovering fraudulent incidents in their accounts would enhance effective detection and prevention capacities and promote the existing banks. However, designing an effective information campaign on customer awareness would require acknowledging and understanding what customers currently know about e-banking fraud and how to detect it. The suggested technique for this research would be a large-scale survey, which would involve all customers of all Nigerian banks as the research population.

The next area of future research concerns synergy among home banks, foreign banks and non-banking organizations in the prevention and detection of fraud. It is obvious that cooperation between banks and non-banking organizations in fighting fraud would enhance the reduction of fraudulent activities in the Nigerian banking industry.

Particularly, the findings of this research have revealed that there is a dependable connection between bank workers and customers, irrespective of whether they are banks or non-banking organizations, which gives a fraud-perpetrating staff member or customer the chance to move unnoticed from one bank and secure a job or commit fraud in another bank or non-banking organization. It is essential, in relation to the lack of resources in the banks and judicial institutions in Nigeria to fight financial fraud, that an opportunity is given to banks to collaborate with other organizations and elevate their capability to prevent and detect fraud.

REFERENCES

Ablon, L., Libicki, M. C., & Golay, A. A. (2014). Markets for cybercrime tools and stolen data. *Rand Corporation.*

Abou-Robieh, M. (2005). *A study of e-banking security perceptions and customer satisfaction issues* (D.B.A.). Available from ProQuest Business Collection. (305340121). Retrieved from http://search.proquest.com/docview/305340121?accountid=10472

Abu-Shanab, E., & Matalqa, S. (2015). Security and fraud issues of E-banking. *International Journal of Computer Networks and Applications (IJCNA), 2*(4), 179-187.

Abu-Shanab, E., & Pearson, J. M. (2009). Internet banking in Jordan: An Arabic instrument validation process. *Int.Arab J.Inf.Technol., 6*(3), 235-244.

Account takeover (2009). Tavistock Square London WC1H 9LT.: The UK's Fraud Prevention Service.

ACFE. (2006). *ACFE report to the nation on occupational fraud and abuse.* (Technical Report). Texas: Association of Certified Fraud Examiners.

ACFE. (2015). *ACFE report to the nation on occupational fraud and abuse.* (). Texas.: Technical Report, Association of Certified Fraud Examiners.

Action Fraud, (2015, 2 December). New figures show steep rise in telephone scams. *Press Release UK Fraud Trends 2015.*

Adams, R. (2010). Prevent, protect, pursue–a paradigm for preventing fraud. *Computer Fraud & Security, 2010*(7), 5-11.

Adedipe, A. A. (2016). Nigerian internet fraud: Policy/Law changes that can improve effectiveness.

Adewumi, O. (1986). "Fraud in banks: An overview. *In Frauds in Banks Chartered Institute of Bankers, Nigeria.*

Adeyemo K. A. (2012). Fraud in Nigerian banks: Nature, deep seated causes, aftermaths and probable remedies. *Mediterranean Journal of Social Sciences, 3*(2), 279-289.

Agbada, A. O., & Osuji, C. (2013). The efficacy of liquidity management and banking performance in Nigeria. *International Review of Management and Business Research, 2*(1), 223-233.

Agboola, A. A. & Salawu, R. O. (2008). Optimizing the use of information and communication technology (ICT) in Nigerian banks. *Journal of Internet Banking and Commerce, 13*(1), 1-15.

Agwu, E. (2012). A qualitative study of the problems and prospects of online banking in developing economies - case of Nigeria. *Journal of Internet Banking and Commerce, 17*(3), 1-20.

Aibieyi .S. (2007). Anti-corruption strategies and development in Nigeria: A case study of the independent corrupt practices commission (ICPC) and economic and financial corruption commission (EFCC). *A Journal of Contemporary Research., 4*, 212-234.

AJAYI, M. A., NAGERI, I. K., ABOGUN, S., & ABDULMUMIN, B. A. (2018). Evaluation of deposit money bank's efficiency in Nigeria: Data envelopment analysis. *Fountain University Osogbo Journal of Management, 2*(1)

Akers, R. (Ed.). (1998). *Social learning and social structure: A general theory of crime and deviance*. Boston: North-eastern University Press.

Akindele, R. I. (2011). Fraud as a negative catalyst in the Nigerian banking industry. *Journal of Emerging Trends in Economics and Management Sciences (JETEMS), 2*(5), 357-363. doi:ournal of Emerging Trends in Ec.

ALAO, A. A. (2016). Analysis of fraud in banks: Evidence from Nigeria. *International Journal of Innovative Finance and Economics Research, 4*(2), 16-25.

Albrecht, C., Turnbull, C., Zhang, Y., & Skousen, C. J. (2010). The relationship between South Korean chaebols and fraud. 33(3), 257-268. *Management Research Review, 33*(3), 257-268.

Albrecht, W. S., Albrecht, C., & Albrecht, C. C. (2008). Current trends in fraud and its detection: A global perspective. *Information Security Journal, 17*, 2-12. doi:10.1080/19393550801934331

Amaratunga, R. G., Baldry, D., Sarshar, M., & Newton, D. (2002). Qualitative and quantitative research in the built environment: Application of "mixed" research approach. *Work Study (Renamed) International Journal of Productivity and Performance Management, 51*(1), 17-31.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioural intentions. *MIS Quarterly, 34*(3), 613-643.

Anderson, K. B. (2006). Who are the victims of identity theft? the effect of demographics. *Journal of Public Policy & Marketing, 25*(2), 160-171.

Anderson, R., Barton, C., Boehme, R., Clayton, R., Levi, M., Moore, T., & Savage, S. (2012). Measuring the cost of cybercrime. Paper presented at the *WEIS Conference,* Berlin.

Anderson, R., Bond, M., & Murdoch, S. J. (2006). Chip and spin. *Computer Security Journal, 22*(2), 1-6.

Anyanwu, C. M. (2010). An overview of current banking sector reforms and the real sector of the Nigerian economy. *Economic and Financial Review, 48*(4), 31-56.

Arrindell, W. A., & Van der Ende, J. (1985). An empirical test of the utility of the observations-to-variables ratio in factor and components analysis. *Applied Psychological Measurement, 9*(2), 165-178.

ASSOCHAM (Ed.). (2015). *Current fraud trends in the financial sector, joint study of associated chambers of commerce and industry of India*. New Delhi: PWC. Retrieved from www.pwc.in

Association of Certified Fraud Examiners. (2010). *Report to the nation on occupational fraud*
. (). Austin, TX: ACFE.

Attrichter, H., Fieldmar, A., Posch, P., & Somekh, B. (2008). Teachers investigate their work. *An introduction to action research across the professions* (Second Edition ed., pp. 147). Routledge: Routledge.

AusCERT (Ed.). (2005). *Australian 2005 computer crime and security survey*. Brisbane: AusCERT.

AusCERT (Ed.). (2006). *Australian 2006 computer crime and security survey*. Brisbane: AusCERT.

Australian Crime Commission. (2004). Parliamentary joint committee on the Australian crime commission 2004. *Cybercrime Canberra Parliament of the Commonwealth of Australia.*

AvinashIngole, & Thool R. C. (2013). Credit card fraud detection using hidden Markov model and its performance. *International Journal of Advanced Research in Computer Science and Software Engineering, 3*(6)

Bagnoli, M., & Watts, S. (2010). Oligopoly, disclosure, and earnings management. *The Accounting Review, 85*(4), 191-1214.

Bahnsen, A. C., Stojanovic, A., Aouada, D., & Ottersten, B. (2013). (2013). Cost sensitive credit card fraud detection using Bayes minimum risk. Paper presented at

the *Proceedings-2013 12th International Conference on Machine Learning and Applications, ICMLA 2013, 1* 333-338.

Bakre, O. (2007). The unethical practices of accountants and auditors and the compromising stance of professional bodies in the corporate world: Evidence from corporate Nigeria. *Accounting Forum, 31*, 277-303.

Banstola, A. (2007). Prospects and challenges of E-banking in Nepal. *The Journal of Nepalese Business Studies, 1*, 96-104.

Barker, K. J., D'Amato, J., & Sheridon, P. (2008). Credit card fraud: Awareness and prevention. *Journal of Financial Crime, 15*(4), 398-410. doi:http://dx.doi.org/10.1108/13590790810907236

Barnett, C. (2002). The measurement of white-collar crime using uniform crime reporting (UCR) data. *US Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services (CJIS) Division.*

Barratt, M. J., Ferris, J. A., & Lenton, S. (2015). Hidden populations, online purposive sampling, and external validity: Taking off the blindfold. *Field Methods, 27*(1), 3-21.

Bartholomew, D. (2008). The rhythm of identity management. *Baseline, 81*, 38-40.

Bartlett, M. S. (1950). Tests of significance in factor analysis. *British Journal of Statistical Psychology, 3*(2), 77-85.

Beard, D., & Wen, H. J. (2007). Reducing the threat levels for accounting information systems. *The CPA Journal, 77*(5), 34-38,40-42.

Beghdad, R. (2008). Critical study of neural networks in detecting intrusions. *Computers & Security, 27*(5-6), 168-175.

Belan, S., Mane, S., & Patani, T. (2014). Fraud detection in online banking using hidden markov model.

Bennett, M. J. (1986). A developmental approach to training for intercultural sensitivity. *International Journal of Intercultural Relations, 10,* 179-195. doi:10.1016/0147-1767(86)90005-2

Bergadano, D., Gunetti, C., & Picardi. (2002). User authentication through keystroke dynamics. *ACM Transactions on Information and System Security, 5*(4), 367-397.

Bernard, H. R. (Ed.). (2006). *Research methods in anthropology*. Lanham: MD: Altamira Press.

Bhasin, M. (2007). The bank internal auditor as fraud buster. *The ICFAI Journal of Audit Practice, 4*(1)

Bhasin, M. L. (2015). Menace of frauds in the indian banking industry: An empirical study. *Australian Journal of Business and Management Research, 4*(2), 21-33.

Bhasin, M. L. (2015). Menace of frauds in the Indian banking industry: An empirical study
. *Australian Journal of Business and Management Research, 4*(2), 21-33.

Bhasin, M. L. (2016). Combatting bank frauds by integration of technology: Experience of a developing country. *British Journal of Research,* doi: ISSN 2394-3718

Bhasin, M. L. (2016). Role of technology in combatting bank frauds: Perspectives and prospects. *International Review of Social Sciences, 4*(1), 21-37.

Bhattacharyya, D., Ranjan, R., Alisherov, F., & Choi, M. (2009). Biometric authentication - A review. *International Journal of u- and e- Service, Science and Technology, 2*(3)

BIS. (2012). 10 steps to cyber security. department for business. *Innovation and Skills,*

BIS. (2012). The 2011 skills for life survey: A survey of literacy, numeracy and ICT levels in England. *Department of Business Innovation and Skills,*

BITS. (2003). Fraud prevention strategies for internet banking, A publication of the BITS fraud reduction steering committee, 17th October,2016.

Blass, A. A., & Oved, Y. (2003). Financing R&D in mature companies: An empirical analysis. *Economics of Innovation and New Technology, 12*(5), 425-447.

Blumberg, B., Cooper, D. R., & Schindler, P. S. (Eds.). (2005). *Business research methods*. Maidenhead: McGraw Hill.

Blumer, H. (Ed.). (1969). *Symbolic interactionism: Perspective and method*. Englewood Cliffs: Prentice Hall.

Blunch, N. (2012). *Introduction to structural equation modeling using IBM SPSS statistics and AMOS* Sage.

Bo, X., & Surya , Y. (2003). (2003). Effect of online reputation service in electronic markets: A trust- based empirical study. Paper presented at the *Ninth Americas Conference on Information Systems,* America.

Bo, X., & Surya, Y. (2003). (2003). Effect of onine reputation service in electronic markets: A trust-based empirical study. Paper presented at the *Ninth Americas Conference on Information Systems. 2003,*

Boechat, G. C., Ferreira, J. C., & Carvalho, E. C. (2006). (2006). Using the keystrokes dynamic for systems of personal security. Paper presented at the *Transactions on Engineering, Computing and Technology,* Enformatika. *18*(1) 200-205.

Boniface, C. (1991). Fraud in the banking industry. the Nigerian banker Oct.-Dec. 22&23. CIBN press.

Bossler, A. M., & Holt, T. J. (2009). Online activities, guardianship & malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology, 3*(1), 400-420.

Bracken, S. (2010). Discussing the importance of ontology and epistemology awareness in practitioner research. *Worcester Journal of Learning and Teaching, 4*

Bradford, W. R. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency, 50*(216) doi:10.1177/0022427811425539

Brar, T. P. S., Sharma, D., & Khurmi, S. S. (2012). Vulnerabilities in e-banking: A study of various security aspects in e-banking. *International Journal of Computing & Business Research, ,* 1-14. doi:2229-6166

Brar, T. P., Sharma, D., & Singh Khurmi, S. (2012). Vulnerabilities in e-banking: A study of various security aspects in e-banking. *International Journal of Computing & Business Research, ,* 1-14.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101.

Braun, V., Clarke, V., & Terry, G. (2014). Thematic analysis. *Qual Res Clin Health Psychol, 24*, 95-114.

Bridges, D., & Smith, R. D. (Eds.). (2007). *Philosophy, methodology and educational research* (1st ed.) Wiley-Blackwell.

Broadman, H. G., & Isik, G. (Eds.). (2007). *Africa's silk road: China and India's new economic frontier.* Washington: DC: World Bank.

Brown, T. A. (2014). *Confirmatory factor analysis for applied research* Guilford Publications.

Browne, M. W., & Cudeck, R. (1993). Alternative ways of assessing model fit. *Sage Focus Editions, 154*, 136-136.

Brunner, A. D., Decressin, J. W., Decressin, J., Hardy, D. C., & Kudela, B. (2004). *Germany's three-pillar banking system: Cross-country perspectives in Europe* International Monetary Fund.

Bryman, A. (2004). Triangulation. In M. Lewis-Beck, A. Bryman & T. F. Liao (Eds.), *Encyclopedia of social science research methods* (). Thousand Oaks: Sage.

Bryman, A. (2006). Integrating quantitative and qualitative research: How is it done. *Qualitative Research, 6*(1), 97-113.

Bryman, A. (2008). methods and methodology. *Qualitative Research in Organizations and Management: An International Journal, 3*(2), 159-168.

BRYMAN, A. (Ed.). (2012). *Social research methods* (4th ed.). Oxford: Oxford University Press.

Bryman, A., & Bell, E. (2015). *Business research methods* Oxford University Press, USA.

Bryman, A., & Bell, E. (Eds.). (2007). *Business research methods* (2nd ed.). Oxford New York: Oxford University Press Inc.

Calderon, T., & Green, B. P. (1994). Internal fraud leaves its mark: Here's how to spot, trace and prevent it. *National Public Accountant, 39*(2), 17-20.

Campbell, D. T., & Fiske, D. W. (1959). Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychological Bulletin, 56*(2), 81-105.

Candy, P. (Ed.). (1991). *Self-direction for lifelong learning.* San Francisco: Jossey-Bass.

Carpenter, T., & Reimers, J. (2005). Unethical and fraudulent financial reporting: Applying the theory of planned behaviour. *Journal of Business Ethics, 60*(2), 115-129.

CBN Annual Report (2016). Financial institutions under the supervisory purview of CBN.

CBN Bank supervision report. (2018). Financial institutions under the supervisory purview of CBN: Deposit money banks, Retrieved from https://www.cbn.gov.ng/supervision/AllFinInstitutions.asp

CBN. (2009). Economic report for the fourth quarter of the *CBN. Collier, P. & A, 4*(4)

Central Bank of Nigeria (CBN). (2002). Financial institutions under the supervisory purview of CBN.

Central Bank of Nigeria (CBN). (2017). Financial institutions under the supervisory purview of CBN.

Central Bank of Nigeria. (2014). Economic report for the first half of 2002. *Abuja: Central Bank of Nigeria,*

Chakrabarty, K. C. (2013). (2013). Fraud in the banking sector – causes, concerns and cures. Paper presented at the *National Conference on Financial Fraud Organised by ASSOCHAM,* New Delhi.

Chakraborty, S. (2013, September 13, 2013). Indian banking set to become fifth largest by 2020: KPMG-CII report. *Business Standard News*

Chan, P. K., Fan, W., Prodromidis, A. L., & Stolfo, S. J. (1999). Distributed data mining in credit card fraud detection. *IEEE Intelligent Systems and their Applications, 14*(6), 67-74.

Chanson, S. T., & Cheung, T. W. (2001). Design and implementation of a PKI-based end-to-end secure infrastructure for mobile e-commerce. *World Wide Web, 4*(4), 235-253.

Chanson, S.T., Cheung, T.W. (2001). Design and implementation of a PKI-based end-to-end secure infrastructure for mobile e-commerce. *World Wide Web, 4*(4), 235-253.

Chartered Institute of Management Accountants. (2008). Fraud risk management: A guide to good practice. *Chartered Institute of Management Accountants,* 1-80.

Chaturvedi, A., & Meena, A. (2016). Analyzing the impacts of phishing and vishing attacks in internet banking. *International Journal of Advanced Research in Computer Science and Software Engineering, 6*(3), 16-21.

Chaudhary, K., Yadav, J., & Mallick, B. (2012). A review of fraud detection techniques: Credit card. *International Journal of Computer Applications (0975 – 8887), 45*(1), 39-44.

Chaudhry, P. E., Chaudhry, S., & Reese, R. (2012). Developing a model for enterprise information systems security. *Economics, Management and Financial Markets, 7*(4), 587-599.

Chen, C. C., Shaw, R. S., & Yang, S. C. (2006). Mitigating information security risks by increasing user security awareness: A case study of an information security

awareness system. *Information Technology, Learning, and Performance Journal, 24*(1), 1-14.

Chen, Y., & Tang, T. L. (2006). Attitude towards and propensity to engage in unethical behaviour: Measurement invariance across major among university students. *Journal of Business Ethics, 69*(1), 77-93.

Chenery, S., Henshaw, C., & Pease, K. (1999). Elegal parking in disabled bays: A means of offender targeting. (briefing note 199.) London, UK: Policing and reducing crime unit, home office research, development and statistics directorate.

Chiemeke, S., Evwiekpaefe, A., & Chete, F. (2006). The adoption of internet banking in Nigeria: An empirical investigation. *Journal of Internet Banking and Commerce, 11*(3), 1-10.

Chiezey, U., & Onu, A. C. (2013). Impact of fraud and fraudulent practices on the performance of banks in Nigeria. *British Journal of Arts and Social Sciences, 15*(1)

Chigada, J., & Ngulube, P. (2015). Knowledge-management practices at selected banks in south Africa. *South African Journal of Information Management, 17*(1), 1-10.

Choo, K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security, 30*(8), 719-731.

Choplin, J. M., & Stark, D. P. (2013). Doomed to fail: A psychological analysis of mortgage disclosures and policy implications. *Banking & Financial Services Policy Report, 32*(10), 11-19.

Chorąś, M., Mroczkowski, P. (2007). (2007). Web security enhancement based on keystroke dynamics. Paper presented at the *Third International Conference on Web Information Systems and Technologies.* doi:10.5220/0001264903370340

CIFAS (Ed.). (2009). ***T****he anonymous attacker: A special report on identity fraud and account takeover*. Tavistock Square London: The UK's Fraud Prevention Service.

CIMA (Ed.). (2009). *Fraud risk management A guide to good practice* (2nd ed.). 26 Chapter Street London SW1P 4NP United Kingdom: The Chartered Institute of Management Accountants, doi:978-1-85971-611-3

Clarke, R. V. (1999). Hot products: Understanding, anticipating and reducing demand for stolen goods (paper 112), B. Webb (ed.). London: Home office, research development and statistics directorate.

Clarke, R. V., & Cornish, D. B. (1985). Modeling offenders' decisions: A framework for research and policy. In M. Tonry, & N. Morris (Eds.), *Crime and justice: A review of research, vol. 6.* (). Chicago, IL: University of Chicago Press.

Clarke, R. V., & Felson, M. (Eds.). (1993). *Routine activity and rational choice, advances in criminological theory.* (Vol.5 ed.). New Brunswick NJ: Transaction Book.

Cohen, L., & Manion, L. (2000). Research methods in education. (5th ed., pp. 254) Routledge.

Cohen, L.E. and Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588-608.

Collins, K. M. T., Onwuegbuzie, A. J., & Sutton, I. L. (2006). A model incorporating the rationale and purpose for conducting mixed-methods research in special education and beyond, learning disabilities. *A Contemporary Journal*, *4*(1), 67-100.

Collis, J., & Hussey, R. (Eds.). (2009). *Business research: A practical guide for undergraduate and postgraduate students* (3rd ed.). New York: Palgrave Macmillan.

Comrey, A. L., & Lee, H. B. (2013). *A first course in factor analysis* Psychology Press.

Conradt, C. (2012). Online auction fraud and criminological theories: The Adrian Ghighina case. *International Journal of Cyber Criminology, 6*(1), 912-923.

Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Worley's critique of situational crime prevention. *Crime Prevention Studies, 16*, 41-96.

Cornish, D. B., & Clarke, R. V. (Eds.). (1986). *The reasoning criminal: Rational choice perspectives on offending* (eds. ed.). New York, NY: Springer-Verlag.

Council, F. F. I. E. (2011). Authentication in an internet banking environment.

Coxon, A. P. (Ed.). (2005). *Integrating qualitative and quantitative data: What does the user need?* (3rd ed.) Open University Press.

Cressey, D. R. (Ed.). (1953). *Other People's money*. Montclair, NJ: Patterson Smith.

Creswell, J. W. (Ed.). (2009). *Research design; qualitative, and mixed methods approaches* (3rd ed.). Sage Publications:

Creswell, J. W., Plano, C. V. L., Gutmann, M. L., & Hanson, W. E. (2003). Advanced mixed methods research designs". In A. Tashakkori, & C. Teddlie (Eds.), *Handbbok*

of mixed methods in social and behavioural research thousand oaks (pp. 209-240) CA: Sage Publications.

Crotty, M. (Ed.). (1998). *The foundations of social research: Meaning and perspective in the research process*. London: Sage Publications.

Crowther, D., & Lancaster, G. (Eds.). *Research methods: A concise introduction to research in management and business consultancy.* (2nd ed.). London: Elsevier Ltd.

Çule, M., & Fulton, M. (2009). Business culture and tax evasion: Why corruption and the unofficial economy can persist. *Journal of Economic Behaviour and Organisation, 73*(3), 811-822.

Curt's carpet services. (2013). (). Costa Mesa, United States, Costa Mesa: Experian Information Solutions, Inc. Retrieved from ABI/INFORM Collection Retrieved from https://search.proquest.com/docview/1587783885?accountid=10472

Dalton, G., & Colombi, J. (2006). (2006). Analyzing attack trees using generalized stochastic petri nets. Paper presented at the *2006 IEEE Workshop on Information Assurance,* NY, USA. 116-123.

Dandash, O., Wang, Y., Leand, D. P., & Srinivasan, B. (2008). Fraudulent internet banking payments prevention using dynamic key. *Journal of Networks, 3*(1), 25-34. doi:10.4304/jnw.3.1.25-34

Darlington, L. (Ed.). (1999). *Banking without boundaries: How the banking industry is transforming itself for the digital age, blueprint for the digital economy.* New York: McGraw Hill.

David, M., and Sutton, C. (2004). Social research: The basics, *Thousand Oaks, CA: Sage,*

Deloitte Fraud Survey. (April 23, 2015). *The Deloitte India banking fraud survey.* (No. Report Edition II). Press Trust of India Report.

Deloitte Survey. (2012, February 8). Indian banking fraud survey. *Business Standard,*

Denning, D. (2000). Reflections on cyberweapons controls. *Computer Security Journal, 16*(4), 3-53.

Denscombe, M. (Ed.). (2008). *The good research guide.* (3rd ed.) Open University Press.

Denzin, N. K. (Ed.). (1978). *Sociological methods: A source book* (2nd ed.) N.Y: McGraw Hill.

Denzin, N. K. (Ed.). (1978). *The research act: A theoretical introduction to sociological methods.* USA: McGraw-Hill, Inc.

Denzin, N. K., & Lincoln, Y. S. (Eds.). (2003). *Strategies of qualitative inquiry*. London: Sage Publications.

DeVellis, R. (1991). Scale development theory and applications. *Applied Research Methods Series, 26*, 51-90.

Diebold, I. (2002). ATM fraud and security: White paper. *New York,*

Dimitrios, M., Dimitrios, C., & Lazaros, S. (2013). An examination of the critical factors affecting consumer acceptance of online banking: A focus on the dimensions of risk. *Journal of Systems and Information Technology, 15*(1), 97-116.

Dionco-Adetayo, E. (2011). In Second Edition (Ed.), *Guide to business research and thesis writing*. Ibadan, Nigeria: Rasmed Publications Limited.

Dorminey, J. W., Fleming, A. S., Kranacher, M., & Riley, R. A.,Jr. (2010). Beyond the fraud triangle. *The CPA Journal, 80*(7), 17-23,3.

Dorminey, J. W., Fleming, A. S., Kranacher, M., & Riley, R. A.Jr. (2012). Financial fraud. *The CPA Journal, 82*(6), 61-65.

Dorminey, J., Fleming, A. S., Kranacher, M., & Riley, R. A.,Jr. (2012). The evolution of fraud theory. *Issues in Accounting Education, 27*(2), 555-579.

Duffield, G., & Grabosky, P. (2001). The psychology of fraud. *Trends and Issues in Crime and Criminal Justice, 199*, 1-6.

Dures, E., Rumsey, N., Morris, M., & Gleeson, K. (2011). Mixed methods in health psychology: Theoretical and practical considerations of the third paradigm. *Journal of Health Psychology, 16*(2), 332-341.

Dzomira, S. (2015). Cyber-banking fraud risk mitigation: Conceptual model. *Banks and Bank System, 10*(2), 7-14.

Dzomira, S. (2015). Online & electronic fraud prevention & safety tips cognizance in south African banks. *Socioeconomical – the Scientific Journal for Theory and Practice of Socio-Economic Development, 4*(8), 527-540. doi: dx.doi.org/10.12803/SJSECO.48131

Easterby-Smith, M., Thorpe, R., & Lowe, A., (Eds.). (2002). *Management research: An introduction, London* (2nd ed.). London: Sage Publication.

Eck, J. E., & Clarke, R. V. (2003). Classifying common police problems: A routine activity approach. *Crime Prevention Studies, 16*, 7-39.

El-Guindy, M. N. (2008). Cybercrime in the middle east Egypt. *SSA Journal,*

ENISA. (2012). National cyber security strategies: Setting the course for national efforts to strengthen security in cyberspace. *European Union Agency for Network and Information Security,*

ENISA. (2014).16 million E-identities and passwords theft. *European Union Agency for Network and Information Security.*

Eskin, E., & Stolfo, S. J. (2007). *System and Methods for Intrusion Detection with Dynamic Window Sizes,*

European Central Bank. (2014). *Third report on card fraud. Third Report on Card Fraud F e b r u a Ry 2014.,*

EveryoneAPI. (2014). Fraud mitigation and identity verification for card not present transactions.

Ezeoha, A. (2007). Structural effects of banking industry consolidation in Nigeria: A review. *Journal of Banking Regulation, 8*(2), 159-176.

Ezeoha, A. E. (2005). Regulating internet banking in Nigeria, problem and challenges (part 1). *Journal of Internet Banking and Commerce, 10*(3)

Fabrigar, L. R., Wegener, D. T., MacCallum, R. C., & Strahan, E. J. (1999). Evaluating the use of exploratory factor analysis in psychological research. *Psychological Methods, 4*(3), 272.

Fatokun, D. (2016). Fraud landscape in Nigeria. *A Changing Payments Ecosystem: The Security Challenge,*

Felson, M. (1995.). Those who discourage crime. In John E. Eck, & W. David (Eds.), *Crime and place: Crime prevention studies* (). Monsey, NY: Criminal Justice Press.

Felson, M. (2008). Routine activity approach. In R. Wortley, & L. Mazzerole (Eds.), *Environmental criminology and crime analysis* (pp. 70-77). New York: Willan Publishing.

Felson, M., & Clarke, R. V. (1998). *Opportunity makes the thief: Practical theory for crime prevention.* (police research series paper 98.) London, UK: Policing and reducing crime unit, home office research, development and statistics directorate.

Felson, M., & Rachel, B. (Eds.). (2010). *Crime and everyday life* (4th ed.) Sage Publications.

Ferguson, E., & Cox, T. (1993). Exploratory factor analysis: A users' guide. *International Journal of Selection and Assessment, 1*(2), 84-94.

Financial Fraud Action UK (FFA UK). (2016). Fraud update: Payment cards, remote banking and cheque. *2016,* May 2016.

Financial Fraud Action UK, (2015, 27 March). Scams and computer viruses contribute to fraud increases – calls for national awareness campaign. *Press Release*

Finch, E. (2010). Strategies of adaptation and diversification: The impact of chip and PIN technology on the activities of fraudsters. *Security Journal,*

Finger, P. T., Tran, H. V., Turbin, R. E., Perry, H. D., Abramson, D. H., Chin, K., . . . Ritch, R. (2003). High-frequency ultrasonographic evaluation of conjunctival intraepithelial neoplasia and squamous cell carcinoma. *Archives of Ophthalmology, 121*(2), 168-172.

Finkle, J., & Hosenball, M. (Eds.). (2014). *FBI warns retailers to expect more credit card breaches.* Reuters.

Fisher, B. S., Daigle, L. E., & Cullen, F. T. (2010). Unsafe in the ivory tower: The sexual victimization of college women. *Thousand Oaks, CA: Sage.,*

Fleetwood, S. (Ed.). (1999). *Critical realism in economics: Development and debate*. London: Routledge.

Ford, N. (2011). Banking security: How to beat the fraudsters. *African Banker,* (15), 20-22,24.

Ford, N. (2015). Fighting the techno criminals. *African Banker,* (31), 34-36.

Frazer, L., & Lawley, M. (2000). Questionnaire design and administration. *A Practical Guide", Milton, QLD: John Wiley and Sons,*

Ganesan, R., & Vivekanandan, K. (2009). A secured hybrid architecture model for internet banking (e-banking). *Journal of Internet Banking and Commerce, 14*(1), 1-17.

Garson, G. D. (2008). Structural equations modelling, from statnotes: Topics in multivariate analysis. *Retrieved on June, 15*

Gates, T., & Jacob, K. (2009). Payments fraud: Perception versus reality. *Economic Perspectives, 33*(1), 7-15.

George, T. K., & Jacob, P. (2015). Fraud detection and mitigation in secure e-payment transaction. *International Journal of Scientific & Engineering Research, 6*(2), 1217-1220. doi:ISSN 2229-5518

Gertler, M., & Nobuhiro, K. (2010). Financial intermediation and credit policy in business cycle analysis. In Friedman, Benjamin M., and Michael Woodford (Ed.), *Handbook of monetary economics* (pp. 547-599). Amsterdam, The Netherlands: Elsevier.

Ghosh, A. K., Schatz, M., Michael, C. C., & Schwartzbard, A. (2007). *Computer Intrusion Detection System and Method Based on Application Monitoring,*

Ghosh, A. K., Schwartzbard, A., & Schatz, M. (1999). (1999). Learning program behavior profiles for intrusion detection. Paper presented at the *Workshop on Intrusion Detection and Network Monitoring, , 51462* 1-13.

Giacinto, G., Roli, F., & Didaci, L. (2003). Fusion of multiple classifiers for intrusion detection in computer networks. *Pattern Recognition Letters, 24*(12), 1795-1803.

Giles, J. (2010). Scareware: The inside story. *New Scientist, 205*(2753), 38-41.

Gillett, P., & Uddin, N. (2005). CFO intentions of fraudulent financial reporting. *Auditing Journal of Practice and Theory, 24*(1), 55-75.

Glorfeld, L. W. (1995). An improvement on horn's parallel analysis methodology for selecting the correct number of factors to retain. *Educational and Psychological Measurement, 55*(3), 377-393.

Gorman, G. E. (2006). What does "online" mean in 2006? *Online Information Review, 30*(5), 481-484. doi:http://dx.doi.org/10.1108/14684520610713822

Gorsuch, R. L. (1997). Exploratory factor analysis: Its role in item analysis. *Journal of Personality Assessment, 68*(3), 532-560.

Gottfredson, M., & Hirschi, T. (Eds.). (1990). *A general theory of crime*. Berkeley, CA: Stanford University Press.

Gottschalk, P. (2010). Categories of financial crime. *Journal of Financial Crime, 17*(4), 441-458.

Grabosky, P., & Smith, R. (2001). Telecommunication fraud in the digital age. *Wall DS* (). London Routledge: Crime and the Internet.

Grabosky, P., Russell, G. S., & Dempsey, G. (Eds.). (2001). *Electronic theft unlawful acquisition in cyberspace*. Cambridge: Cambridge University Press.

Graham, J. R., Li, S., & Qiu, J. (2008). Corporate misreporting and bank loan contracting. *Journal of Financial Economics, 89*, 44-61.

Graycar, A., & Smith, R. (2002). (2002). Identifying and responding to electronic fraud risks. Paper presented at the *30th Australasian Registrars' Conference Canberra,*

Greene, J. C. (2008). Is mixed methods social inquiry a distinctive methodology? *Journal of Mixed Methods Research, 2*(1), 7-22.

Greene, J. C., Caracelli, V. J., & Graham, W. F. (1989). Towards a conceptual framework for mixed-method evaluation designs. *Educational Evaluation and Policy Analysis, 11*(3), 255-274.

Grix, J. (Ed.). (2004). *The foundations of research.* London: Macmillan.

Gunathilake, N., Padikaraarachchi, A., Koralagoda, S., Jayasundara, M., Paliyawadana, P., Manawadu, C., & Rajapaksha, U. (2013). Enhancing the security of online banking systems via keystroke dynamics. Paper presented at the *Computer Science & Education (ICCSE), 2013 8th International Conference on*, 561-566.

Gunetti, D., & Picardi, C. (2005). Keystroke analysis of free text. *ACM Transactions on Information and System Security (TISSEC), 8*(3), 312-347.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (Eds.). (2010). *Multivariate data analysis: A global perspective.* (7th ed.) New Jersey: Pearson Prentice Hall.

Hair, J., Money, A., Page, M., & Samouel, P. (Eds.). (2007). *Research methods for business* (First Edition ed.). The Atrium, Southern Gate, Chichester, West Sussex PO198SQ, England: John Wiley & Son Ltd. doi:978-0-470-03404-0

Halfpenny, P. (1997). The relationship between quantitative and qualitative social research. *Bulletin De Methodologie Sociologique, 57*, 49-64.

Hamilton, D. I., Justin, M., & Odinioha, G. (2012,). Dimensions of fraud in Nigeria quoted firms. *American Journal of Social and Management Sciences, 3(3)*(2156-1540 2151-1559), : 112-120. doi:10.5251/ajsms.2012.3.3.112.120

Hammersley, M. (1996). The relationship between qualitative and quantitative research: Paradigm loyalty versus methodological eclecticism. In J. E. T. Richardson (Ed.), *Handbook of qualitative research methods for psychology and the social sciences* [ ] (pp. 159-174). Leicester: British Psychological Society.

Hansen, J., McDonald, J., Messier, W., & Bell, T. (1996). A generalized qualitative-response model and the analysis of management fraud. *Management Science, 42*, 1022-1033.

Harrell, E., & Lynn, L. (Eds.). (2013). *Victims of identity theft, 2012*. Bulletin NCJ 243779: U.S. Department of Justice Bureau of Justice Statistics.

Harwood, T. G., & Garry, T. (2003). An overview of content analysis. *The Marketing Review, 3*(4), 479-498.

Hayton, J. C., Allen, D. G., & Scarpello, V. (2004). Factor retention decisions in exploratory factor analysis: A tutorial on parallel analysis. *Organizational Research Methods, 7*(2), 191-205.

Henn, M., Weinstein, M., & Foard, N. (Eds.). (2009). *A short introduction to social research*. London: Sage Publications.

Hill, M. R. (1984). Epistemology, axiology, ideology in sociology. *Mid-American Review in Sociology, 9*(2), 59-77.

Ho, R. (Ed.). (2006). *Handbook of univariate and multivariate data analysis and interpretation with SPSS*. London: Chapman and Hall/ CRC.

Hoang, X. D., Hu, J., & Bertok, P. (2003). (2003). A multi-layer model for anomaly intrusion detection using program sequences of system calls. Paper presented at the *11th IEEE International Conf. Networks*, 531-536.

Hoehle, H., Scornavacca, E., & Huff Sid. (2012). Three decades of research on consumer adoption and utilization of electronic banking channels: A literature analysis.*54*(1), 122-132. doi:http://doi.org/10.1016/j.dss.2012.04.010

Hoffman, D. G. (Ed.). (2002). *Managing operational risk: 20 firmwide best practice strategies.* London: John Wiley and Sons.

Holden, M. T., & Lynch, P. (2004). *choosing the appropriate methodology understanding research philosophy.* (). Waterford: Waterford Institute of Technology.

Holden, M. T., & Lynch, P. (Eds.). (2004). *Choosing the appropriate methodology understanding research philosophy.* Waterford.: Waterford Institute of Technology.

Hollinger, R. D., & Clark, J. P. (Ed.). (1983). *Theft by employees.* Lexington: Lexington Books.

Hollis-Peel, M. E., Reynald, D. M., van Bavel, M., Elffers, H., & Welsh, B. C. (2011). Guardianship for crime prevention: A critical review of the literature. *Crime, Law and Social Change, 56*(1), 53-70.

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimisation', deviant behaviour, (30), 1-25.

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior, 30*(1), 1-25.

Holt, T. J., & Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimisation. *Deviant Behavior, 30*(1), 25.

Holtfreter, K. (2005). Is occupational fraud "typical" white-collar crime? A comparison of individual and organisational characteristics. *Journal of Criminal Justice, 33*, 353-365.

Holtfreter, K., Beaver, K. M., Reisig, M. D., & Pratt, T. C. (2010). Low self-control and fraud offending. *Journal of Financial Crime, 17*(3), 295-307. doi:http://dx.doi.org/10.1108/13590791011056264

Hooks, K. L., Kaplan, S. E., Schultz, J. J.,Jr, & Ponemon, L. A. (1994). Enhancing communication to assist in fraud prevention and detection; comment: Whistle-blowing as an internal control mechanism: Individual and organizational considerations. *Auditing, 13*(2), 86.

Horn, R. (Ed.). (2010). *Designing A trading system*. CC Suite 509, Private Bag X503 Northway, 4065, KZN, ZA: Alaziac Trading CC Nominee Old Tree Publishing.

Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives, 6 (1) p.p. 155, 1999. *Structure Equation Modelling, 6*(1), 155.

Hutcheson, G. D., & Sofroniou, N. (1999). *The multivariate social scientist: Introductory statistics using generalized linear models* Sage.

Hutchings, A., & Hayes, H. (2009). Routine activity theory and phishing victimisation: Who gets caught in the 'Net'? *Current Issues in Criminal Justice, 20*(3), 433-451.

Ibor, B. I. (2016). An empirical investigation of the human resources nexus to frauds in the nigerian banking sector. *International Journal of Scientific and Research Publications, 6*(6), 231-247.

Idowu, A., & Adedokun, T. O. (l2013). Evaluation of the effect of monitoring and control activities on fraud detection in selected Nigerian commercial banks. *Research Journal of Finance and Accounting, .4*(6), 37-54.

Igbaekemen, G. O., Abbah, M. T., & Geidam, M. M. (2014). The effect of corruption on socio-economic development of Nigeria. *Canadian Social Science, 10*(6), 149-157.

IIA, AICPA, & ACFE. (2015). Managing the business risk of fraud: A practical guide.

Imala, O. (2001). The impact of the previously liquidated Banks/Financial institutions and the efficacy of the measures put in place by the supervisory and the regulatory. *Authorities. A Paper Presented at the Public Hearing on Developments in the Banking. System Organized by House Committee on Banking and Currency, Abuja, June, 1*

Imiefoh, P. (2012). Towards effective implementation of electronic banking in Nigeria. *African Research Review, 6*(2), 290-300.

Imiefoh, P. (2012). Towards effective implementation of electronic banking in Nigeria. *African Research Review, 6*(2), 290-300.

Iminza, N. W., Gikiri, W. l., & Kiragu, D. N.,. (2015). Operational governance and occupational Fraud Risk in commercial banks in Kenya. *European Journal of Business Management, 2*(1), 401-442.

Iwuagwu, O. (2000). Corruption: A threat to democracy and national development. *Journal of National Economic Group of Nigeria, 8*(1), 12-16.

Jackson, C., Barth, A., Bortz, A., Shao, W., & Boneh, D. (2009). Protecting browsers from DNS rebinding attacks. *ACM Transactions on the Web (TWEB), 3*(1), 2.

Jakobsson, M. (2005). (2005). Modeling and preventing phishing attacks. Paper presented at the *Financial Cryptography, 5*

James, F., Stratman, T., Duffy, M. (1990). Conceptualizing research on written management communication looking through a glass onion. *Management Communication Quarterly: McQ (1986-1998), 3*(4), 429.

Jamieson, R., Stephens, G., & Winchester, D. (2007). An identity fraud model categorising perpetrators, channels, methods of attack, victims and organisational impacts. Paper presented at the *Pacific Asia Conference on Information Systems (PACIS) 2007 Proceedings,*

Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to

victimization
. *International Journal of Cyber Criminology*, *10*(1), 79-91. doi:10.5281/zenodo.58523

Jassal, R. K., & Sehgal, R. K. (2013). Online banking security flaws: A study. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*(8), 1016-1021.

Jeffords, R., Marchant, M. L., & Bridendall, P. H. (1992). How useful are the tread way risk factors? *Internal Auditor*, 60-62.

Jenkins, H. W.,Jr. (2004, Apr 14, 2004). Business world: Is corporate fraud too hard for juries? *Wall Street Journal*, pp. A.15. Retrieved from http://search.proquest.com/docview/398911418?accountid=10472

Johnson, M. (2008). *Johnson, M. (2008). A new approach to internet banking.* . (Unpublished PhD Thesis). University of Cambridge, Cambridge, UK. Retrieved from http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-731.pdf (731)

Johnston, A. (2014). Rigour in research: Theory in the research approach. *European Business Review*, *26*(3), 206-217. doi:http://dx.doi.org/10.1108/EBR-09-2013-0115

Kadushin, C., Sasson, T., & Saxe, L. (2008). Triangulation and mixed methods designs: Practicing what we preach in the evaluation of an Israel Experience educational program. *SAGE Journals Online and High Wire Press Platforms*, *20*(1),46-65. doi:10.1177/1525822X07307426

Kaiser, M. (1974). Kaiser-Meyer-Olkin measure for identity correlation matrix. *Journal of the Royal Statistical Society*, *52*, 296-298.

Kanu, S. I., & Okorafor, E. O. (2013). The nature, extent and economic impact of fraud on bank deposits in Nigeria. *Interdisciplinary Journal of Contemporary Research in Business*, *4*(9), 253-265.

Karlsen, K. N., & Killingberg, T. (2008). Profile based intrusion detection for internet banking systems. *Norwegian University of Science and Technology*,

Karmen, A. (Ed.). (2010). *Crime victims: An introduction to victimology*. Belmont, CA: Cengage Wadsworth Learning.

Kassem, R., & Higson, A. (2012). The new fraud triangle model. *Journal of Emerging Trends in Economics and Management Sciences*, *3*(3), 191-195.

KATHIRVEL, K. (2013). Credit card frauds and measures to detect and prevent them. *International Journal of Marketing, Financial Services & Management Research, 2*(3), 172-179.

Keivani, F. S., Jouzbarkand, M., Khodadadi, M., & Sourkouhi, Z. K. (2012). (2012). A general view on the E-banking. Paper presented at the *International Proceedings of Economics Development & Research, ,43*

Keivani, F. S., Jouzbarkand, M., Khodadadi, M., & Sourkouhi, Z. K. (2012). (2012). A general view on the E-banking. Paper presented at the *International Proceedings of Economics Development & Research, , 43*

Kelling, G. L., Pate, T., Dieckman, D., & Brown, C. E. (1974). *The Kansas city preventive patrol experiment.* (A Summary Report No. Catalog Number 74-24739). 1201 Connecticut Avenue, NW, Suite 200 Washington, DC 20036-2636: Police Foundation. Retrieved from http://www.policefoundation.org/docs/copyright.html Retrieved from www.policefoundation.org

Kemper, E. A., Stringfield, S., & Teddlie, C. (2003). Mixed methods sampling strategies in social science research. *Handbook of Mixed Methods in Social and Behavioral Research, ,* 273-296.

Kemper, E. A., Stringfield, S., & Teddlie, C. (2003). Mixed methods sampling strategies in social science research. *Handbook of Mixed Methods in Social and Behavioral Research, ,* 273-296.

Kennedy, L. W., & Forde., D. R. (1990). Routine activities and crime: An analysis of victimization in Canada. *Criminology, 28*(1), 137-151.

Kevin Wang, S., & Huang, W. (2011). The evolutional view of the types of identity thefts and online frauds in the era of the internet. *Internet Journal of Criminology, ,* 1-21. doi:2045-6743

Khin, E. W. S., & Heng, T. N. (2012). Epistemological taxonomy in management & accounting research philosophy. *Actual Problems of Economics, 131*(330), 338.

Kimani, W. (2013,). EAC banks grapple with fraud cases. *Daily Nation, Smart Company*, pp. 2-3.

Kinkela, K., & Harris, P. (2014). ACFE releases 2014 international study on internal fraud investigation, advocating internal audit. *Internal Auditing, 29*(5), 10-14.

Kiolbassa, K., Miksch, A., Hermann, K., Loh, A., Szecsenyi, J., Joos, S., & Goetz, K. (2011). Becoming a general practitioner-which factors have most impact on career choice of medical students? *BMC Family Practice, 12*(1), 25.

Kirda, E., & Kruegel, C. (2006). Protecting users against phishing attacks. *The Computer Journal, 49*(5), 554-561.

Kline, P. (2014). *An easy guide to factor analysis* Routledge.

Kocsis, R. (Ed.). (2006). *Criminal profiling: principals and practice*. NJ: Humana Press.

Kolapo, T. F., Ayeni, R. K., & Oke, M. O. (2012). Credit risk and commercial banks'performance in Nigeria: A panel model approach. *Australian Journal of Business and Management Research, 2*(2), 31.

Kothari, C. R. (2004). *Research methodology: Methods and techniques* New Age International.

Kothari, C. R. (Ed.). (2004). *Research methodology: Methods and techniques* (Second Edition ed.). 4835/24, Ansari Road, Daryaganji, New Delhi- 110002: New Age International (P) Limited, Publishers. doi:NSBN (13) :978-81-224-2488-1

Kothari, C. R., & Garg, G. (Eds.). (2014). *Research methodology: Methods and techniques* (3RD ed.). 4835/24, Ansari Road, Daryaganji, Delhi-110002: New Age International (P) Limited, Publishers. doi:978-81-224-3623-5

Kou,Y., Lu,C.,and Sirwongwattana, S. (2004)). Survey of fraud detection techniques. *In 2004 International Conference on Network, Sensing and, Control, ,* 749-754.

Kovach, S., & Ruggiero, W. V. (2011). (2011). Online banking fraud detection based on local and global behavior. Paper presented at the *The Fifth International Conference on Digital Society,* Guadeloupe, France. 166-171.

KPMG Forensic. (2006). *Guide to preventing workplace fraud. Taking action to reduce business crime exposure.*

KPMG. (2000). E-commerce and cybercrime: New strategies for managing the risks of exploitation. *Forensic and Litigation Services, KPMG LLP, USA, ,* 27 March 2015.

KPMG. (2005, African fraud and misconduct survey.

KPMG. (2012). Government and public-sector cybercrimes. *A Financial Sector View,*

Krambia-Kapardis, M. (2002). A fraud detection model: A must for auditors. *Journal of Financial Regulation and Compliance, 10*(3), 266-278.

Kranacher, M. J., Riley, R. A., & Wells, J. T. (Eds.). (2011). *Forensic accounting and fraud examination*. London: John Wiley and Sons.

Krauss, S. E. (2005). Research paradigms-qualitative report article. *The Qualitative Report, 10*(4), 758-770.

Lancaster, G. (Ed.). (2005). *Research methods in management* (First ed.). Linacre House, Jordan Hill, Oxford OX2 8DP, 30 Corporate Drive, Burlington, MA01803: Elsevier Butterworth- Heinemann. doi:0750662123 Retrieved from http://www.elsevier.com

Langenderfer, J., & Shimp, T. (2001). Consumer vulnerability to scams, swindles and fraud: A new theory of visceral influences on persuasion. *Psychology & Marketing, ,* 763-769.

Laurens, R., & Zou, C. C. (2016). (2016). Using Credit/Debit card dynamic soft descriptor as fraud prevention system for merchant. Paper presented at the *Global Communications Conference (GLOBECOM), 2016 IEEE,* 1-7.

Lawson, T. (Ed.). (2004). *A conception of ontology*. Cambridge: University of Cambridge Press.

Ledesma, R. D., & Valero-Mora, P. (2007). Determining the number of factors to retain in EFA: An easy-to-use computer program for carrying out parallel analysis. *Practical Assessment, Research & Evaluation, 12*(2), 1-11.

Ledesma, R. D., & Valero-Mora, P. (2007). Determining the number of factors to retain in EFA: An easy-to-use computer program for carrying out parallel analysis. *Practical Assessment, Research & Evaluation, 12*(2), 1-11.

Leukfeldt, E. R. (2014). Phishing for suitable targets in the netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking, 17*(8), 551-555.

Leukfeldt, E. R. (2014). Phishing for suitable targets in the netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking, 17*(8), 551-555.

Leukfeldt, E. R. (2014). Phishing for suitable targets in the netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking, 17*(8), 551-555.

Leung, A., Yan, Z., & Fong, S. (2004). (2004). On designing a flexible e-payment system with fraud detection capability. Paper presented at the 236-243.

Levi, M., & Williams, M. L. (2013). Multi-agency partnerships in cybercrime reduction: Mapping the network and cooperation space. *Information Management and Computer Security, 21*(fadayomatthew@yahoo.com), 420-443.

Lewis, C. (2011). *Empowering regulators to protect consumer rights in the ICT sector: Final*
technical report. ().

Lindner, J. R., Murphy, T. H., & Briers, G. E. (2001). Handling nonresponse in social science research. *Journal of Agricultural Education, 42*(4), 43-53.

Lister, L. M. (Ed.). (2007). *A practical approach to fraud risk: Internal auditors.*

Loehline, J. C. (Ed.). (1987). *Latent variable structural models: An introduction to factor path, and structural analysis*. Hillsdale NJ: Lawrence Erlbaum Associates, Inc.

Longo, E., & Stapleton, J. (2002). (2002). PKI note: Smart cards. . *PKI Note Series, PKI Forum,*

Loonam, M., & O'Loughlin, D. (2008). An observation analysis of e-service quality in online banking. *Journal of Financial Services Marketing, 13*(2), 164-178.

Losee, J. (Ed.). (1993). *A historical introduction into the philosophies of science* (3rd ed.). Oxford: Oxford University press.

Lynch, J. (2005). Identity theft in cyberspace: Crime control methods and their effectiveness in combating phishing attacks. *Berkeley Technology Law Journal, 20*, 259-300.

Mac, F. (2015). *Fraud Mitigation Best Practices, January,*

MacCallum, R. C., Widaman, K. F., Zhang, S., & Hong, S. (1999). Sample size in factor analysis. *Psychological Methods, 4*(1), 84.

MacGibbon, A. (Ed.). (2005). *Australian e-commerce safety guide* Sydney eBay.

Mahdi, M. D. H., Rezaul, K. M., & Rahman, M. A. (2010). (2010). Credit fraud detection in the banking sector in UK: A focus on e-business. Paper presented at the *Paper Presented at the Proc. of the 4th International Conference on Digital Society (ICDS '10),* St. Maarten. 232-237.

Mahdi, M. D. H., Rezaul, K. M., & Rahman, M. A. (2010). (2010). Credit fraud detection in the banking sector in UK: A focus on e-business. Paper presented at the *Proc. of the 4th International Conference on Digital Society (ICDS '10),* St. Maarten. 232-237.

Manyika, J., & Roxburgh, C. (2011). The great transformer: The impact of the internet on economic growth and prosperity. *McKinsey Global Institute,*

Marascuilo, L. A., & Levin, J. R. (1983). *Multivariate statistics in the social sciences: A researcher's guide* Wadsworth Publishing Company.

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory. *Deviant Behaviour, 31*(5), 381-410. doi:10.1080/01639620903004903

Marsh, H. W., & Hocevar, D. (1985). Application of confirmatory factor analysis to the study of self-concept: First-and higher order factor models and their invariance across groups. *Psychological Bulletin, 97*(3), 562.

Masocha, R., Chiliya, N., & Zindiye, S. (2011). E-banking adoption by customers in the rural milieus of south africa: A case of alice, eastern cape, south africa. *African Journal of Business Management, 5*(5), 1857-1863. doi:http://dx.doi.org/10.5897/AJBM10.850

Mhamane, S. S., & Lobo L m r j. (2012). Use of hidden markov model as internet banking fraud detection. *International Journal of Computer Applications, 45*(21) doi:10.5120/7071-9556

Mhamane, S. S., & Lobo, L. M. R. (2012). (2012). Internet banking fraud detection using HMM. Paper presented at the *icccnt'12,* Coimbatore, India. IEEE-20180.

Miesch, A. (1975). Variograms and variance components in geochemistry and ore evaluation. *Geological Society of America Memoir, 142*, 333-340.

Miles, M. B., & Huberman, A. M. (Eds.). (1994). *Qualitative data analysis: An expanded source book* . London: Sage Publications.

Miller, J. (2013). Individual offending, routine activities, and activity settings: Revising the routine activity theory of general deviance. *Journal of Research in Crime and Delinquency, 50*(3), 390-416.

Miller, J. M. (Ed.). (2014). *The encyclopedia of theoretical criminology (vol. 1).* John Wiley & Sons.

Mirjana Pejic-Bach (Ed.). (2010). *Profiling intelligent systems applications in fraud detection and prevention: Survey of research articles*

Mitchell, M., & Jolley, J. (2004). Measuring and manipulating variables: Reliability and validity. *Research Design Explained 5th Edition (Pp, 104 & 536),*

Monrose, F., & Rubin, A. (2000). Keystroke dynamics as a biometric for authentication . *International Journal of Future Generation Computer Systems, 16*(4), 351-359. doi:PII: S0167-739X(99)00059-X

Moore, T., & Clayton, R., & Anderson, R. (2009). The economics of online crime 23 (3), 3-20. *The Journal of Economic Perspectives, 23*(3), 3-20.

Moskovitch, R., Feher, C., Messerman, A., Kirschnick, N., Mustafic, T., Camtepe, A., . . . Elovici, Y. (2009). Identity theft computers and behavioral biometrics. intelligence and security Informatics . *ISI '09. IEEE International Conference on,* doi:10.1109/ISI.2009.5137288

Mroczkowski, P., & Choras, M. (2006). (2006). Keystroke dynamics in biometrics client-server password hardening system. Paper presented at the *Advanced Computer Systems (ACS),* Miedzyzdroje, Poland. , *2* 75-82.

Murdoch, S., & Anderson, R. (2010). Verified by visa and MasterCard SecureCode: How not to design authentication. In R. Sion (Ed.), *Financial cryptography and data security* (6052nd ed., pp. 336-342). Heidelberg: Springer Berlin.

Muscat, G., James, M., & Graycar, A. (2002). Older people and consumer fraud, *Trends and Issues in Crime and Criminal Justice, 220,* 1-6.

Nahar, A., Roy, S., & Hasan, S. S. (2016). A survey on different approaches used for credit card fraud detection. *International Journal of Applied Information Systems (IJAIS), 10*(4), 31-34.

Nance, W. D., & Straub, D. W. (1988). An investigation into the use and usefulness of security software in detecting computer abuse, (eds), , pp. 283-294. In J.I. DeGloss, & M. H. Olson (Eds.), *Proceedings of the ninth international conference on information systems* (pp. 283-294). MN: Minneapolis.

Narekar, Y. M., & Chavan, S. K. (2015). A review on credit card fraud Detection Using BLAST-SSAHA Method. *International Journal of Advanced Research in Computer and Communication Engineering, 4*(11), 425-433.

NDIC. (2012). *Annual reports and statement of accounts.* ().Nigeria Deposit Insurance Corporation.

NDIC. (2012). *Nigeria deposit insurance corporation (NIDC) annual.* (Annual Report).

Nedelescu, M., & Stănescu, C. (2012). Produse şi servici bancare. *Editura Universitară, Bucureşti,*

NeFF. (2016). A changing payments ecosystem: The security challenge. *Annual Report, 2016,*

Neuman, L. W., & Neuman, W. L. (Eds.). (2000). *Social research methods quantitative and qualitative approaches* (4th ed.) Allyn & Bacon. doi:13: 9780205297719

Newman, C. J., & Neier, D. S. (2014). Become proactive, not reactive, to anti-fraud and anti-corruption programs. *Financial Executive, 30*(4), 14-16.

Newman, G., & Clarke, R. V. (Eds.). (2003). *Superhighway robbery: Preventing E-commerce crime.* . Portland, Willan Publishing.

NIBSS, & Diamond Bank. (2015, 10 April). The evolution of the Nigerian payment system. *POS Adoption Study-Lagos State,* , 8-9.

Nigerian Deposit Insurance Scheme (NDIC). (2008-2011). Annual reports and statement of accounts.

Njenga, N. M., & Osiemo. (2013). Effect of fraud risk management on organization performance: A case of deposit-taking microfinance institutions in Kenya. *International Journal of Social Sciences and Entrepreneurship, 1*(7), 1-17.

Njenga, N.Osiemo (2013). effect of fraud risk management on organization performance: A case of deposit-taking microfinance institutions in Kenya. *International Journal of Social Sciences and Entrepreneurship, 1*(7), 490-507.

Nkemdili, N. A., Bonaventure, U., & Kingsley, A. (2013). No light at the end of the tunnel: Corruption and insecurity in Nigeria. *Arabian Journal of Business and Management Review (Oman Chapter), 2*(12), 41-54.

Nor, K. M., Shanab, E. A. A., & Pearson, J. M. (2008). Internet banking acceptance in Malaysia based on the theory of reasoned action. *JISTEM-Journal of Information Systems and Technology Management, 5*(1), 03-14.

Norse (Ed.). (2014). *Account takeover: A complex and growing problem* Norse Corporation.

Nunnally, J. (1978). Psychometric methods. 2nd Edition, McGraw-Hill, New York.

Nunnally, J. C., & Bernstein, I. (1994). *Psychometric theory (McGraw-hill series in psychology)* McGraw-Hill New York.

Nwankwo, O. (2013). Implications of fraud on commercial banks performance in nigeria. *International Journal of Business and Management, 8*(15), 144-150.

Nwaze, C. (Ed.). (2006). *Bank fraud exposed with cases and preventive measures*. Lagos: Control and Surveillance Associates Ltd.

Obalola, M. A. (2010). *Ethics and social responsibility in the Nigerian insurance industry: A multi-methods approach.* (Unpublished Doctoral thesis). De Montfort University, Leicester, UK.

Odediran, O. (2014). Holistic approach to electronic channels fraud management. *Nigeria Electronic Fraud Forum (NeFF) 2014 Annual Report,*

Odusami, M. (2015). 3 party cyber risk management using security ratings to manage cyber risk. In Nigerian e-Fraud Forum (NeFF), & Central Bank of Nigeria (CBN) (Eds.), *The 2015 annual report , NeFF: Improving and securing the cyber-environment* (pp. 40-52)

Office for National Statistics. (2015). Crime in England and wales. *Year Ending December 2014,*

Ogbuji, C. N., Onuoha, C. B., & Izogo, E. E. (2012). Analysis of the negative effects of the automated teller machine (ATM) as a channel for delivering banking services in nigeria. *International Journal of Business and Management, 7*(7), 180-190.

Oghenerukevbe, E. A., DME. (2008). Customers perception of security indicators in online banking sites in nigeria. *Journal of Internet Banking and Commerce, 13*(3), 1-14.

Oghenerukeybe, E. A., DME. (2009). Customers perception of security indicators in online banking sites in Nigeria. *Journal of Internet Banking and Commerce, 14*(1), 1-15.

Ojo. (2008). Effect of frauds on banking operations in Nigeria. *International Journal of Investment and Finance, 1*(1), 103.

Oko, S., & Oruh, J. (2012). Enhanced ATM security system using biometrics. *International Journal of Computer Science Issues (IJCSI), 9*(5), 352.

OKOH, J. I., & OKOH, J. O. (2020). Banking sector reforms in Nigeria and unemployment implications. *Government, University of Nigeria, Nsukka,* , 116.

Olaoye, C. O., & Adekola, D. R. (2014). Analysis of frauds in banks: Nigeria's experience. *European Journal of Business and Management, 6 (31)*(2222-1905; 2222-2839), 90-99.

Olawale, F., & Garwe, D. (2010). Obstacles to the growth of new SMEs in south africa: A principal component analysis approach. *African Journal of Business Management, 4*(5), 729-738.

Olodude, O. (2015). *Ransomware: An evolving threat.* (The NeFF 2015 Annual Report). Central Bank of Nigeria (CBN). (NeFF: Improving and Securing the Cyber Environment)

Olsen, W. K. (2004). Triangulation in social research: Qualitative and quantitative methods can really be mixed. In M. Holborn, & U. Haralambos (Eds.), *Developments in sociology* () Causeway Press. doi:d093fbb8-6c02-4915-9d90-907d8c82105d

Omar, A. B., Sultan, N., Zaman, K., Bibi, N., Wajid, A., & Khan, K. (2011). Customer perception towards online banking services: Empirical evidence from pakistan. *Journal of Internet Banking and Commerce, 16*(2), 1-24.

Omariba, Z., Masese, N., & Wanyembi, G. (2012). Security and privacy of electronic banking. *IJCSI International Journal of Computer Science, 9*(3), 432-446.

Ombudsman. (2015). *Calling time on telephone fraud a review of complaints about "vishing" scams.* (Financial Ombudsman Service insight report). United Kingdom: Financial Ombudsman Service Limited.

Omotayo, T. and Kulatunga, U. (2015). (2015). The research methodology for the development of a kaizen costing frame-work suitable for indigenous construction firms in lagos, Nigeria. . Paper presented at the *ARCOM Doctoral Workshop Research Methodology,* Grange Gorman Campus, Dublin Institute of Technology.

Omoteso, K. (2006). *The impact of information communication technology on auditing.* (Unpublished PhD Thesis). De Montfort University, United Kingdom.

Online banking frauds in India cause us$1.3mln in 2009 losses. (2011, Aug 5, 2011). *Asia Pulse,* pp. n/a. Retrieved from http://search.proquest.com/docview/881769564?accountid=10472

Onwuegbuzie, A. J., Leech, N. L., & Collins, K. T. (2012). Qualitative analysis techniques for the review of the literature. *The Qualitative Report, 17*(56), 1-28.

Orakci, Ş., & Toraman, Ç. (2018). The validity and reliability studies of the scale attitude toward pedagogical teacher training programme. *MOJES: Malaysian Online Journal of Educational Sciences, 6*(3), 49-61.

Orji, V., O. (2015). Knowledge management systems: Issues, challenges, and benefits. *Communications of the Association for Information Systems, 1*(7)

Owolabi S. A. (2010). Fraud and fraudulent practices in Nigerian banking industry. *African Research Review, 4*(3), 240--256.

Owolabi, A. (2011). Corruption and the environment of accounting and auditing in Africa. *International Journal of Critical Accounting, 3*(1-3) doi:10.1504/IJCA.2011.039752

Paler-Calmorin, L., & Calmorin, M. A. (2007). *Research methods and thesis writing* Rex Book Store.

Pallant, J. (2001). *SPSS survival manual: A step by step guide to data analysis using SPSS for windows (versions 10 and 11):* SPSS student version 11.0 for *windows* Open University Press Milton Keynes.

Pallant, J. (2005). SPSS survival manual: A step by step guide to data analysis using SPSS for windows (version.)

Pallant, J. (2010). SPSS survival manual: A step by step guide to data analysis using SPSS . maidenhead.

Pallant, J. (2013). *SPSS survival manual* McGraw-Hill Education (UK).

Pallant, J. (Ed.). (2007). *SPSS survival manual. a step by step guide to data analysis using SPSS for windows*. UK: McGraw Hill.

Palmerino, M. B. (1999). Take a quality approach to qualitative research. *Marketing News, 33*(12), 35-36.

Pandey, M., (2010). A model for managing online fraud risk using transaction validation. *The Journal of Operational Risk, 5*(1), 49-63.

Pandy, S. (2016). Mitigating fraud risk in the card-not-present environment. *Federal Reserve Bank of Boston,*

Pandy, S. (Ed.). (2016). *Payment strategies: Mitigating fraud risk in the card-not-Present1 environment* Federal Reserve Banks of Boston and Atlant.

Papazoglou, M. P. (2003). Web services and business transactions. *World Wide Web, 6*(1), 49-91.

Park, S. (2015). *Winning the online banking war*. Blackhat USA: TrendMicro.

Parliamentary Joint Committee on the Australian Crime Commission (2004). Cybercrime Canberra parliament of the commonwealth of Australia.

Patil, R. A., & Renke, A. L. (2016). Keystroke dynamics for user authentication and identification by using typing rhythm. *International Journal of Computer Applications (0975 – 8887), 144*(9)

Patton, M. Q. (Ed.). (1990). *Qualitative evaluation and research methods* (2nd ed.). London: Sage Publications.

Pedneault, S., Silverstone, H., Rudewicz, F., & Sheetz, M. (2012). *Forensic accounting and fraud investigation for non-experts* John Wiley & Sons.

Peotta, L., Holtz, M., David, B., Deus, F., & Sousa Jr, R. (2011). A formal classification of interest banking attacks and vulnerabilities. *International Journal of Computer Science & Information Technology (IJCSIT), 3*(1), 186-197.

Perkins, E. D., & Annan, J. (2013). Factors affecting the adoption of online banking in Ghana: Implications for bank managers. *International Journal of Business and Social Research (IJBSR), 3*(6), 94-108.

Perlroth, N., & Gelles, D. (Eds.). (2014). *Russian hackers amass over a billion internet passwords.* . New York: New York Times.

Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. *ArXiv Preprint arXiv:1009.6119,*

Piazza, P. (2005). Defending networks against targeted trojans. *Security Management, 49*(9), 52-52,54.

Polonsky, M. J., & Waller, D. S. (2005). *Research project: Designing and managing a business student guide.* 2455 Teller Road Thousand Oaks, California 91320: Sage Publications Inc. doi:0-76192249-0

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency, 47*(3), 267-296.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency, 47*(3), 267-296.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency, 47*(3), 267-296.

Rae, K., & Subramaniam, N. (2008). Quality of internal control procedures: Antecedents and moderating effect on organisational justice and employee fraud. *Managerial Auditing Journal, 23*(2), 104-124.

Rajdeepa B., & Nandhitha D. (2015). Fraud detection in banking sector using data mining. *International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064, 4*(7), 1822-1825.

Rampini, A. A., & Viswanathan, S. (2010). Collateral, risk management, and the distribution of debt capacity, journal of finance.*65*, 2293-2322.

Rampini, A. A., & Viswanathan, S. (2015). Financial intermediary capital. *Working Paper, Duke University,*

Raykov, T., & Penev, S. (2001). The problem of equivalent structural equation models: An individual residual perspective. *New Developments and Techniques in Structural Equation Modeling,* , 297-321.

Regha, O. (2015). Cybercrime: A risk information centre to the rescue. *Nigeria Electronic Fraud Forum (NeFF) 2015 Annual Report,* , 72-77.

Reisinger, Y., & Mavondo, F. (2007). Structural equation modeling: Critical issues and new developments. *Journal of Travel & Tourism Marketing, 21*(4), 41-71.

Revett, K. (2009). A bioinformatics-based approach to user authentication via keystroke dynamics. *International Journal of Control, Automation, and Systems, 7*(1), 7-15. doi:http://dx.doi.org/10.1007/s12555-009-0102-2

Revett, K., De Magalhães, S. T., & Santos, H. M. (2005). Password secured sites stepping forward with keystroke dynamics. in next generation web services practices. . Paper presented at the *NWeSP 2005. International Conference on IEEE.*

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency, 50*(2), 216-238.

Reyns, B. W., & Henson, B. (2013). *Security in a Digital World: Understanding and Preventing Cybercrime Victimization,*

Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International Journal of Offender Therapy and Comparative Criminology, 60*(10), 1119-1139.

Reyns, B., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlife style-routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior, 38*(11), 1149-1169.

Roberds, W. (1998). The impact of fraud on new methods of retail payment. *Economic Review - Federal Reserve Bank of Atlanta, 83*(1), 42-52.

Rocco, T. S., Bliss, L. A., Gallagher, S., & Perez-prado, A. (2003). Taking the next step: Mixed methods research in organizational systems. information technology. *Learning and Performance Journal, 21*(1), 19-29.

RSA (2010) A monthly intelligence report from the RSA anti-fraud command centre. (online fraud report).

Sahin, Y., & Duman, E. (2010). (2010). An overview of business domains where fraud can take place, and a survey of various fraud detection techniques. Paper presented at the *1st International Symposium on Computing in Science and Engineering,* Aydin, Turkey.

Saleh, Z. (2013). The impact of identity theft on perceived security and trusting E-commerce. *Journal of Internet Banking and Commerce, 18*(2), 1-11.

Saleh, Z. I. (2011). Improving security of online banking using RFID. *Academy of Banking Studies Journal, 10*(2), 1.

Salim, H. (Ed.). (2014). *Cyber safety: A systems thinking and systems theory approach to managing cyber security risks*. Massachusetts Institute of Technology Cambridge: Composite Information Systems Laboratory (CISL) Sloan School of Management. doi:MA 02142

Salu, A. O. (2004). Online crimes and advance fee fraud in Nigeria - are available legal remedies adequate? *Journal of Money Laundering Control, 8*(2), 159-167.

Sanusi, L. (2010). The Nigerian banking industry: What went wrong and the way forward. *Delivered at Annual Convocation Ceremony of Bayero University, Kano Held on, 3*(1), 2010.

Sanusi, S. L. (2011). Banking reform and its impact on the Nigerian economy. *CBN Journal of Applied Statistics, 2*(2), 115-122.

Sanusi, S. L. (2011). Global financial meltdown and the reforms in the Nigerian banking sector. *CBN Journal of Applied Statistics, 2*(1), 93-108.

Saranya, K. & Gunasri, K. (2013). Challenges in E-banking. *International Journal of Scientific Research and Management (IJSRM),* (22), 27.

Sarma, G., & Singh, P. K. (2010). Internet banking: Risk analysis and applicability of biometric technology for authentication. *International Journal of Pure and Applied Sciences and Technology, 1*(2), 67-78.

Saudi, M. M., Ismail, S., Tamil, E. M., & Idris, M. Y. I. (2007). Phishing: Challenges and issues in malaysia. *International Journal of Learning, 14*(8), 79-88.

Saunders, M. L. and Thornhill P. (2003). *Research Methods for Business Students,*

Saunders, M., Lewis, P., & Thornhill, A. (2009). Understanding research philosophies and approaches. *Research Methods for Business Students, 4*, 106-135.

Saunders, M., Lewis, P., & Thornhill, A. (Eds.). (2007). *Research methods for business students* (4th Edition ed.). Edinburgh Gate, Harlow, Essex CM20 2JE, England: Pearson Education Limited. doi:13-978-0-273-70148-4 Retrieved from www.pearsoned.co.uk

Saunders, M., Lewis, P., & Thornhill, A. (Eds.). (2015). *Research methods for business students* (Seventh ed.). Edinburgh Gate, Harlow, Essex CM20 2JE, England: Pearson Education Limited. doi:978-1-292-01662-7 Retrieved from www.pearson.com/uk

Saunders, M., Lewis, P., & Thronhill, A. (Eds.). (2012). *Research methods for business students* (4th ed.). Harlow: Pearson Education Ltd.

Schneier, B. (2011). *Secrets and lies: Digital security in a networked world* John Wiley &Sons.

Schumacker, R. E., & Lomax, R. G. (2012). *A beginner's guide to structural equation modeling* Routledge.

Schumacker, R. E., & Lomax, R. G. (Eds.). (2004). *A beginner's guide to structural equation modeling*. Mahwah, N.J: Lawrence Erlbaum Associates.

Schutt, R. K. (Ed.). (2003). *Investigating the social world: The process and practice of research*. Newbury Park: CA: Pine Forge Press.

Sekaran, U. (Ed.). (2003). *Research methods for business: A skill building approach* (Fouth ed.). Jose Ortega/Stock Illustration Source: Hermitage Publishing Services, doi:0-471-38448-8; 0-471-2036606

Sekaran, U., & Bougie, R. (Eds.). (2010). *Research methods for business: A skill building approach* (Fifth Edition ed.). The Atrium, Southern Gate, Chichester, West Sussex, PO198SQ, United Kingdom: John Wiley & Sons Ltd. doi:978-470-74479-6

Sekaran, U., & Bougie, R. (Eds.). (2013). *Research methods for business: A skill-building approach* (Sixth Edition ed.). The Atrium, Southern Gate, Chichester, West Sussex, PO198SQ, United Kingdom: John Wiley & Son Ltd. doi:978-1-118-52785-6 Retrieved from www.wileyopenpage.com

Shah, M. (2009). *E-banking management: Issues, solutions, and strategies: Issues, solutions, and strategies* IGI Global.

Shah, M. H., Braganza, A., & Morabito, V. (2007). A survey of critical success factors in e-banking: An organisational perspective. *European Journal of Information Systems, 16*(4), 511-524. doi:http://dx.doi.org/10.1057/palgrave.ejis.3000693

Shanmugapriya, D., & Padmavathi, G. (2009). A survey of biometric keystroke dynamics: Approaches, security and challenges. *International Journal of Computer Science and Information Security, IJCSIS, 5*(1), 115-119. doi:ISSN 1947 5500

Shannak, R. O. (2013). Key issues in E-banking strengths and weaknesses. *The Case of Two Jordanian Banks, European Scientific Journal, 9*(7), 239-263.

Silverstone, H., & Sheetz, M. (Eds.). (2007). *Forensic accounting and fraud investigation for non-experts* (2nd ed.). New Jersey, USA: John Wiley & Sons, Inc.

Singh, P., & Singh, M. (2015). Fraud detection by monitoring customer behavior and activities. *International Journal of Computer Applications (0975 – 8887), 111*(11), 23-32.

Singh, Y. K. (Ed.). (2006). *Fundamental of research methodology and statistics* (1ST ed.). 4835/24, Ansari Road, Daryaganji, New Delhi-110002: New Age International. Publishers. doi:ISBN : 978-81-224-2418-8.

Smith, R. (2007). Biometric solutions to identity-related cybercrime' in jewkes Y (ed) crime online Devon Willan publishing. ()

Smith, R., & Akman, T. (2008). Raising public awareness of consumer fraud in Australia. *Trends and Issues in Crime and Criminal Justice, 349*, 1-6.

Snyder, J. M. (2000). Online auction fraud: Are the auction houses doing all they should or could to stop online fraud? *Federal Communications Law Journal, 52*(2), 453-472.

Soltani, B. (2014). The anatomy of corporate fraud: A comparative analysis of high profile American and European corporate scandals. *Journal of Business Ethics, 120*(2), 251-274. doi:http://dx.doi.org/10.1007/s10551-013-1660-z

Srivastava, A., Kundu, A., Sural, S., & Majumdar, A. (2008). Credit card fraud detection using hidden markov model. *IEEE Transactions on Dependable and Secure Computing, 5*(1), 37-48.

Srivastava, Abhinav, Amlan, K., Shamik, S., & Arun, K. M. (2008). Credit card fraud detection using Hidden markov model. *IEEE Transactions on Dependable and Secure Computing, 5*(1), 37-48.

Sruthi T.V., & Prasanna. (2016). Fraud detection in banking institutions. *International Journal of Engineering and Technology (IJET), 8*(2), 1127-1130.

Sruthi, T., & Prasanna. (2016). Fraud detection in banking institutions. *International Journal of Engineering and Technology (IJET), 8*(2), 1127-1130. doi:p-ISSN : 2319-861

Stemler, S. (2001). An overview of content analysis. *Practical Assessment, Research & Evaluation, 7*(17), 137-146.

Subramanian, R. (Ed.). (2014). *Bank fraud: Using technology to combat losses*. Carry, North Carolina, USA.: SAS institute Inc.

Suleiman, G. P., Kamariah, M., Adesiyan, O. I., Mohammed, A. S., & Jamal, A. (2012). Customer loyalty in e-banking: A structural equation modelling (SEM) approach. *American Journal of Economics, ,* 55-59. doi:10.5923/j.economics.20120001.13

Sullivan, R. J. (2014). Controlling security risk and fraud in payment systems. *Economic Review - Federal Reserve Bank of Kansas City, ,* 5-36.

Sutton, M. (2009). Product design: CRAVED and VIVA. In B. S. Fisher, & Lab S. P. (Eds.), *Encyclopedia of victimology and crime prevention* (). Sage: Thousand Oaks.

Sydney, I. F. (1986). "Management control system, prevention and detection of frauds. *A Paper Presented at the Seminar on Frauds in Banks Organized by the Nigerian Institute of Bankers, Lagos, Nigeria,*

Symantec Security Response. (2005). (2005). "Phishing in the middle of the stream" - Today's threats to online banking. Paper presented at the *The AVAR 2005 Conference,* Symantec Security Response, Dublin. 1-28.

Symantec. (2015). ISTR 20: Internet security threat report.*20*

Tabachnick, B. G., & Fidell, L. S. (Eds.). (2007). *Using multivariate statistics* (5th ed.). Boston: Allyn and Bacon.

Tan, T. M., & Rasiah, D. (2011). A review of online trust branding strategies of financial services industries in Malaysia and Australia., *Advances in Management & Applied Economics, International Scientific Press, 1*(1), 125-150.

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education, 2*, 53-55. doi: ijme.2.5355 [pii]

Taylor, J. (Ed.). (2011). *Forensic accounting.* (1st ed.). Edinburg Gate Harlow Essex CM20 2JE, England: Pearson education.

Teoh, S. T., Ma, K., Wu, S. F., & Jankun-Kelly, T. (2004). Detecting flaws and intruders with visual data analysis. *IEEE Computer Graphics and Applications, 24*(5), 27-35.

Tessier, D. R. (2013). **T**he fraud triangle theory: how a three-pronged approach can improve your bottom line. *The CLM.*

Tewksbury, R., & Mustaine, E. E. (2001). Lifestyle factors associated with the sexual assault of men: A routine activity theory analysis. *The Journal of Men's Studies, 9*(2), 153-182.

Thamizhchelvy, K., & Geetha, G. (2012). E-banking security: Mitigating online threats using message authentication image (MAI) algorithm. *International Conference on Computing Sciences, ,* 176-284. doi:10.1109/ICCS.2012.29

The World Bank. (2015). Information communications technology for development. *2015 LIMA Annual Meeting, Wor;Ld Bankn Group , International Monetory Funds,*

Tilley, N. (2009). *Crime prevention: criminal justice series* (Illustrated ed.). Pennsylvania State University: Willan Publishing.

Tillyer, M. S., & Eck, J. E. (2009). Routine activities. In J. M. Miller (Ed.), *21st century criminology: A reference handbook* (pp. 279-287). Thousand Oaks: CA: Sage.

Tillyer, M. S., & Eck, J. E. (2010). Getting a handle on crime: A further extension of routine activities theory. *Security Journal. Online First Edition,* doi:10.105710.1057

Tongco, M. D. C. (2007). Purposive sampling as a tool for informant selection. *Ethnobotany Research and Applications, 5,* 147-158.

Tran, V. M., & Perry, J. A. (2003). Challenges to using neem (azadirachta indica var. sianensis valenton) in Thailand. *Economic Botany, 57*(1), 93.

Trochim, W. K., & O'Donnelly, J. P. (Eds.). (2006). *The research methods knowledge base* . (3rd ed.). New York: Thomson.

Tseloni, A., Wittebrood, K., Farrell, G., & Pease, K. (2004). Burglary victimization in England and Wales, the united states and the Netherlands: A cross national comparative test of routine activities and lifestyle theories. *British Journal of Criminology, 4*(1), 66-91.

Uchenna, C., & Agbo J. C. (2013). Impact of fraud and fraudulent practices on performance of banks in Nigeria. *British Journal of Arts and Social Science, 15*(1)

Udoayang, J. O., James, F. U. (2004). Auditing and investigation. *Calabar: University of Calabar Press.,*

Udofia, E. P. (Ed.). (2011). *Applied statistics with multivariate methods*. Enugu: Immaculate Publications Ltd.

Ulbrich, I., Canagaratna, M., Zhang, Q., Worsnop, D., & Jimenez, J. (2009). Interpretation of organic components from positive matrix factorization of aerosol mass spectrometric data. *Atmospheric Chemistry and Physics, 9*(9), 2891-2918.

Ureche, O., & Plamondon, R. (2000). Digital payment systems for internet commerce: The state of the art. *World Wide Web, 3*(1), 1-11.

US-CERT. (2015). Federal incident reporting guidelines. *Official Website of the Department of Homeland Security,*

Usman, A. K., MSc, & Shah, M. H., PhD. (2013). Critical success factors for preventing e-banking fraud. *Journal of Internet Banking and Commerce, 18*(2), 1-15.

Usman, A. K., MSc, & Shah, M. H., PhD. (2013). Strengthening E-banking security using keystroke dynamics. *Journal of Internet Banking and Commerce, 18*(3), 1-11.

Van Wilsem, J. (2013). "Bought it, but never got it" assessing risk factors for online consumer fraud victimization. European sociological review. *Oxford: Oxford Univ Press,* doi:10.1093/esr/jcr053

Vandommele, T. (2010). Biometric authentication today. *Seminar on Network Security,* doi: T-110.5290

Vasiu, L. (2004). (2004). A conceptual framework of eFraud control in an integrated supply chain. Paper presented at the *Proceedings of European Conference on Information Systems (ECIS),* 161-174.

Velicer, W. F., & Fava, J. L. (1998). Effects of variable and subject sampling on factor pattern recovery. *Psychological Methods, 3*(2), 231.

Velicer, W. F., Eaton, C. A., & Fava, J. L. (2000). Construct explication through factor or component analysis: A review and evaluation of alternative procedures for determining the number of factors or components. *Problems and solutions in human assessment* (pp. 41-71) Springer.

Vrincianu, M., & Popa, L. (2010). Considerations regarding the security and protection of E-banking services consumers' interests. . *Journal of Internet Banking and Commerce, 12*(28), 388-403.

Wada, F., & Odulaja G.O. (2012). Electronic banking and cybercrime in Nigeria: A theoretical policy perspective on causation. *African Journal of Computer and ICTs, 5*(1), 69-82.

Wada, F., & Odulaja, G. (2012). Assessing cybercrime and its impact on e-banking in Nigeria using social theories. *African Journal of Computing & ICT, 5*(1), 69-82.

Wada, F., & Odulaja, G. (2012). Electronic banking and cybercrime in Nigeria-A theoretical policy perspective on causation. *African Journal of Computing & ICT Www.Ajocict.Net, 4*(3), 69-82.

Wang, S. K., & Huang, W. (2011). The evolutional view of the types of identity thefts and online frauds in the era of the interne. *Internet Journal of Criminology, ,* 1-14.

Wang, W. Y. C., Rashid, A., & Chuang, H. (2011). Toward the trend of cloud computing. *Journal of Electronic Commerce Research, 12*(4), 238.

Wang, W., Yuan, Y., & Archer, N. (2006). A contextual framework for combating identity theft, IEEE security and privacy. . *IEEE Computer Society,*

Webb, E. J., Campbell, D. T., Schwartz, R. D., & Sechrest, L. (Eds.). (1966). *Unobtrusive measures: Nonreactive research in the social sciences*. Chicago: Rand McNally.

Wei, W., Li, J., Cao, L., Ou, Y., & Chen, J. (2012). Effective detection of sophisticated online banking fraud on extremely imbalanced data. *World Wide Web (Internet and Web Information Systems), ,* 1-29. doi:10.1007/s11280-012-0178-0

Wells, J. (Ed.). (2014). *Corporate fraud handbook: Prevention and detection* (2nd ed.). London: John Wiley and Sons.

Wells, J. T. (2002). Occupational fraud: The audit as deterrent. *Journal of Accountancy, 193*(4), 24-28.

Wells, J. T. (Ed.). (2005). *New approaches to fraud deterrence*. The Institute of Chartered Accountants of India, New Delhi: The Chartered Accountant. doi:1453-1455

Wells, J. T. (Ed.). (2011). *Corporate fraud handbook: Prevention and detection* (3rd ed.). Hoboken, New Jersey: John Wiley & Sons Inc.

Wells, J. T. (Ed.). (2014). *Principles of fraud examination* (4th ed.). United State of America: John Wiley &Sons. Inc. doi:978-1-118-58288-6; 10987654321

Wesley, K. (2004). Fraud management lifecycle theory. A holistic approach to Fraud Management. *Journal of Economic Crime Management, 2*(2)

Wilcox, P., Madensen, T. D., & Tillyer, M. S. (2007). Guardianship in context: Implications for burglary victimisation risk and prevention', , 44: 771–803. *Criminology,* (44), 771-803.

Wilhelm, W. K. (2004). The fraud management lifecycle theory: A holistic approach to fraud management. *Journal of Economic Crime Management, 2*(2), 1-38.

Williams, B., Onsman, A., & Brown, T. (2010). Exploratory factor analysis: A five-step guide for novices. *Australasian Journal of Paramedicine, 8*(3)

Williams, M. L. (2015). Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. *British Journal of Criminology, 56*(1), 21-48.

Williams, M. L., & Levi, M. (2012). Perceptions of the eCrime controllers: Modelling the influence of cooperation and data source factors Security. Journal, doi:10.1057/sj.2012.47.

Wilmot, A. (2005). Designing sampling strategies for qualitative social research: With particular reference to the office for national statistics' qualitative respondent register. *Survey Methodology Bulletin-Office for National Statistics-, 56*, 53.

Wilsem van, J. A. (2013). Bought it, but never got it: Assessing risk factors for online consumer fraud victimization. *European Sociologic Review, 29*(2), 168-178.

Wisdom, K. (2012). *The impact of electronic banking on service delivery to customers of Ghana commercial bank limited* (Ph.D. Thesis,).

Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal, 74*(12), 38-42.

World Bank. (Ed.). (2014). *Cyber security: A model for protecting the network* World Bank.

Wothke, W. (2000). Longitudinal and multi-group modeling with missing data. In T. D. Little, K. U. Schnabel & J. Baumert (Eds.), *Modeling longitudinal and multiple*

group data: Practical issues, applied approaches and specific examples (). Mahwah, New Jersey: Lawrence Erlbaum Associates.

Wothke, W. A. (1993). Wothke, W. A. (1993). nonpositive definite matrices in structural modeling. in (eds.), (pp. 256– 293). . [3, 4, 5, 9. In K. A. Bollen, & Long J. S. (Eds.), *Testing structural equation models* (). Newbury Park,: CA: Sage.

Wright, R. (2007). Developing effective tools to manage the risk of damage caused by economically motivated crime fraud. *Journal of Financial Crime, 14*(1), 17-27.

Yan, A. W., Md-Nor, K., Abu-Shanab, E., & Sutanonpaiboon, J. (2009). Factors that affect mobile telephone users to use mobile payment solution. *International Journal of Economics and Management, 3*(1), 37-49.

Yan, W. N., & Chiu, D. K. (2007). (2007). Enhancing e-commerce processes with alerts and web services: A case study on online credit card payment notification. Paper presented at the *Machine Learning and Cybernetics, 2007 International Conference on, , 7* 3831-3837.

Yar, M. (2005). The novelty of 'Cybercrime' an assessment in light of routine activity theory. *European Journal of Criminology, 2*(4), 407-427.

Yar, M. (2005). The novelty of cybercrime: An assessment in light of routine activity theory. , 2(4), 407–427. *European Journal of Criminology, 2*(4), 407-427.

Yazdanifard, R., WanYusoff , W. F., Behora, A. C., & Abu Bakar Sade. (2011). Electronic banking fraud; the need to enhance security and customer trust in online banking. *International Journal in Advances in Information Sciences and Service Sciences, 3*(10.61), 505-509.

Zahra, S., Priem, R., & Rasheed, A. (2005). The antecedents and consequences of top management fraud. *Journal of Management, 31*(6), 803-828.

Zhang, W., Zhang, Y., & Kim, T. (2014). Detecting bad information in mobile wireless networks based on the wireless application protocol. *Computing. Archives for Informatics and Numerical Computation, 96*(9), 855-874. doi:http://dx.doi.org/10.1007/s00607-013-0325-1

Zimucha, T., Zanamwe, N., Chimwayi, K., Chakwizira, E., Mapungwana, P., & Maduku, T. (2012). An evaluation of the effectiveness of E-banking security strategies in Zimbabwe: A case study of Zimbabwean commercial banks. *Journal of Internet Banking and Commerce, 17*(3), 1-16.

Appendices

Appendix 1: Letter of Introduction and Questionnaires

dmu.ac.uk
DE MONTFORT UNIVERSITY
LEICESTER

31 March, 2017

To Whom It May Concern

Letter of Introduction for Research Data Collection:

Mr. Matthew Oluwalami Fadayo

I write as the supervisor of Matthew and confirm that he is registered on our doctoral programme in the Department of Accounting & Finance, Faculty of Business & Law, De Montfort University, Leicester, United Kingdom. The proposed title of his thesis is, "An Appraisal of E-banking Frauds: Detection and Prevention in Nigerian Banks". He has made steady progress in reviewing the literature and designing his research. He is now ready to start collecting data.

According to the University Research Regulations, he has systematically addressed ethical issues, including assuring confidentiality to the respondents, where it is requested or where there is a possibility of repercussion on the respondent. In the thesis itself, all references to the respondents would be anonymised. He is bound by oath to follow the University's code of ethics. I, therefore, have no hesitation in requesting you to kindly support his research effort and please afford all the possible co-operation.

Yours sincerely,

DE MONTFORT UNIVERSITY SIGILLUM 1861

Dr. Kemi Yekini BSc MSc ACA CFE FHEA PhD
Director Centre for Research in Accountability Governance and Sustainability
Research Coordinator Accounting and Finance

Department of Accounting and Finance, Leicester Business school, HU1.74 Hugh Aston Building, The Gateway, LE1 9BH.
Tel: +44 (0) 116 207 8783, Fax: +44 (0) 116 250 6043, Email: kyekini@dmu.ac.uk

Appendix 2: Questionnaire for the Bank Staff

AN EXAMINATION OF E-BANKING FRAUD PREVENTION AND DETECTION IN NIGERIAN BANKS

SECTION A: Demographic Data	
Instruction: Please, mark the appropriate box for the option that best describes you.	
1	Gender: Male ○ Female ○
2	Age (years): Below 20 ○ 20-30 ○ 31-40 ○ 41-50 ○ 51 and Above ○
3	Highest Educational Qualification: BSc/HND ○ MSc/MBA/MPhil ○ PhD ○
4	Professional Qualification: ACCA ○ ICAN ○ ACIA ○ ANAN ○
5	Number of years in the present establishment 1-4 ○ 5-8 ○ 9-12 ○ 13&above ○
6	What is your current position? .....
SECTION B: THE TOP AND CURRENT E-BANKING FRAUDS IN NIGERIA BANKING INDUSTRY Please, mark your level of agreement with the statement below.	
The following are the top and current e-banking fraud incidents in Nigerian banks:	

S/N	Strongly Agreed (5), Agreed (4), Undecided (3), Disagreed (2), Strongly Disagreed (1)	5	4	3	2	1
B1	Internet Banking Fraud is a current e-banking fraud of high concern to Nigerian banks.					
B2	Identity Fraud is a current e-banking fraud of high concern to Nigerian banks.					
B3	Credit and Debit Card Fraud is a current e-banking fraud of high concern to Nigerian banks.					
B4	Automated Teller Machine Fraud is a current e-banking fraud of high concern to Nigerian banks.					
B5	E-cheque Fraud is a current e-banking fraud of high concern to Nigerian banks.					
B6	Phishing and Pharming Fraud are current e-banking fraud of high concern to Nigerian banks.					

SECTION C: Factors Contributing to the Increase of E-banking Frauds in Nigeria
Please, mark your level of agreement with the statement below.

The following are the top reasons for increase of e-banking fraud incidents in Nigerian banks:

S/N	**Strongly Agreed (5), Agreed (4), Undecided (3), Disagreed (2), Strongly Disagreed (1)**	**5**	**4**	**3**	**2**	1
C1	Pressure to meet business and personal target					
C2	Inadequate fraud detection tools					
C3	Collusion between employees and externals parties					
C4	Lost cards, stolen personal identification data					
C5	Changes to business strategies without changes in business procedures					

C6	Introduction of new products without adequate control and training in place					
C7	Lack of a fraud risk framework within the organization					
C8	Difficulty integrating data from various sources					
C9	Difficulty investigating crimes across borders					
C10	Irregular electricity power supply in Nigeria					
C11	Lack of forensic accounting professionals					
C12	Downloading, browsing, chatting and spending long time on social media					
C13	Weak litigation support in prosecution process					
C14	Lack of oversight by senior management on deviations from existing procedure					
C15	Issuing of counterfeit credit cards by the employees of the issuer's company					
C16	System with virus, weak software, lack of antivirus, weak password and the similar					
C17	Lack of customers and staff unawareness to the fraud incidence					
C18	Lack of dedicated technology tools for investigation and insufficient resources					
C19	Poor coordination with law enforcement					
C20	Lack of effective and efficiency internet network facilities					
C21	Absence quality forensic analysis					
C22	Use of the same password for different accounts					
C23	Lack of rule of law					
C24	Poor system administration and ineffectiveness maintenances					
C25	Lack of forensic accounting professionals and absence of quality forensic analysis					
C26	Lack of dedicated technology tools for investigation					
C27	Insufficient financial resources					
C28	Infectiveness of law enforcement agency					

SECTION D: E-Banking Frauds Prevention in Nigerian Banking Industry

The following fraud management measures need to be implemented effectively by Nigerian banking industry in order to prevent e-banking frauds incidents:

S/N	Strongly Agreed (5), Agreed (4), Undecided (3), Disagreed (2), Strongly Disagreed (1)	5	4	3	2	**1**
D1	Corporate code of conduct					
D2	Carrying out of internal investigation					
D3	Dedicated forensic technology tools for investigation					
D4	Intelligence gathering mechanism					
D5	Employment of bank verification number (BVN) and background check					
D6	Use of token card, PINsentry card, passcode, memorable word					
D7	Collaboration with government, regulators, law enforcement, academia and other partners					
D8	American Express SafeKey, MasterCard SecureCode and Verified by Visa					
D9	Automated Address Verification Service (AVS)					
D10	Checking for cards that are being used fraudulently enhances					
D11	Fraud awareness training,					
D12	Employee background check					
D13	Fraud control strategies, regulations, Internal control policies and prosecution					
D14	Reporting the incident to a law enforcement agency					
D15	Asking the individual in question to resign.					
D16	Upgradation of technology to combat fraud					
D17	Fraud risk assessment					
D18	Fraud control organization structure					
D19	Clearly define reporting structure					
D20	Dedicated fraud investigative team from CBN					

D21	Use of personal identification number and automatic phone call with registered phone number					
D22	Card Security Code (CSC)					
D23	Third party due diligence					
D24	Customer screening against negative list					
D25	Whistle-blower hotline policy					
D26	Data mining					
D27	**Corporate governance**					

SECTION E: Mechanisms of E-banking Fraud Detection in Nigerian Banking Industry

The following are the major means of discovering e-banking fraud in Nigerian Banking Industry:

S/N	Strongly Agreed (5), Agreed (4), Undecided (3), Disagreed (2), Strongly Disagreed (1)	5	4	3	2	**1**
E1	E-banking frauds are detected through customers' complaints.					
E2	Automated data analysis and transaction monitoring software are important tools of detecting e-banking frauds.					
E3	Online reconciliation of account enhances e-banking fraud detection.					
E4	Fraud risk assessments and investigations is a best means of detecting e-banking frauds.					
E5	Fraud detection and monitoring system is an important strategy of detecting e-banking frauds.					
E6	Use of CCTV at point of transaction is a significant tool of detecting e-banking frauds in Nigerian banks.					
E7	E-banking frauds are detected through monitoring of the internet to detect and close malware in the banking industries.					
E8	E-banking frauds are detected through implementation of banking verification number (BVN) approach.					
E9	E-banking frauds are detected through application of computer forensic and forensic accounting approaches.					
E10	E-banking frauds are uncovered through internal whistle-blowers.					
E11	E-banking frauds are uncovered through effective response plan					
E12	E-banking frauds are detected through data mining					
E13	E-banking frauds are detected through fraud controls, monitoring and analysis team					
E14	E-banking frauds are detected through monitoring the phishing-related websites					
E15	E-banking frauds are uncovered through anonymous complaints.					
E16	E-banking frauds are detected through use of fraud detective system software					
E17	E-banking frauds are detected through internal surveillance equipment.					
E18	E-banking frauds are detected through ATM monitoring surveillance					
E19	E-banking frauds are detected through internal and external auditors					
E20	**E-banking frauds are detected through law enforcement agents**					

Appendix 3: Questionnaire for the Banks' Customers

AN EXAMINATION OF E-BANKING FRAUD PREVENTION AND DETECTION IN NIGERIAN BANKS

SECTION A: DEMOGRAPHIC DATA

Instruction: Please, mark the appropriate box for the option that best describes you.

1	Gender: Male ○ Female: ○
2	Age (years): 18- 25 ○ 26-35 ○ 36-45 ○ 46-55 ○ 56 &Above ○
3	H.Edu.Q.: SSCE/OND/NCE ○ BSc/HND ○ MSc/MBA ○ PhD ○

SECTION B: The Determinant Factors of Increase in Electronic Banking Frauds in Nigerian.

Please, mark your level of agreement with the statement below

S/N	rongly Agreed (5), Agreed (4), Undecided (3), Disagreed (2), Strongly isagreed (1)	5	4	3	2	1
A1	I have one bank account					
A2	I have two bank accounts					
A3	I have three bank accounts					
A4	I have four bank accounts					
A5	I have more than four bank accounts					
B1	I have one bank card					
B2	I have two bank cards					
B3	I have three bank cards					
B4	I have four bank cards					
B5	I have more than four bank cards					
C1	I use online banking service regularly					
C2	I use bank card with POS service regularly					
C3	I use ATM fund transfer service regularly					
C4	I use mobile banking service regularly					
C5	I use Phone banking service regularly					
D1	I received my account bank statement regularly					
D2	I check my e-banking account balance regularly					
E1	I use one password for one bank account					
E2	I use only one password I have for all my bank accounts and social media					
E3	I use different passwords for all my bank accounts					
F0	Nigerian banks offer e-banking fraud prevention and detection seminars to their customers regularly					
G0	Customers' awareness of e-banking fraud prevention and detection will have positive impact on mitigation of e-banking frauds.					

Appendix 4: Qualitative Questionnaire for the bank Staff

QUALITATIVE QUESTIONS FOR BANK STAFF	
1	How long have you been working in this banking and What position are you holding?
2	Since when you have been working in this bank, have you observed any online banking fraud incident and what are the kinds of online banking fraud you observed currently?
3	What are the current fraud risks that are of high concern to the Nigerian commercial banks?
4	In your own opinion, what are the contributing factors to the rise in online banking fraud in Nigerian commercial banks?
5	How are the fraud incidents that involved your bank typically detected and what kind of dedicated fraud detection/ analytics solution to identify red flags will you encourage your bank to implemented?
6	In your own opinion, how do you view government's regulations to prevent and detect online banking fraud and how do you view online banking fraudsters prosecuted?
7	What do the preventive mechanism do your bank employ against online fraud and how effective the following preventive mechanism in your bank?
	i. Understanding roles, policy, corporate governance and responsibilities
	ii. Ongoing fraud awareness programme
	iii. Prosecution and Judicial System
	iv. Periodic fraud risk assessment
8	What was the nature of the non-financial loss that your bank suffered, due to the incident of online banking fraud and the challenges faced in the prevention and the detection of online banking fraud in Nigeria commercial banks?
9	What extent is the BVN, an effective tool for e-banking fraud detection and prevention?
10	What are the types of e-banking fraud that have been reduced after the introduction of BVN?

Appendix 5: Communalities

	Initial	Extraction
Difficulty investigating crimes across borders (BA1)	1.000	.847
Insuring of counterfeit bank cards (BA2)	1.000	.965
Collusion between employees and outsiders (BA3)	1.000	.933
Difficulty integration from various sources and lack of effective and efficiency internet network facilities (BA4)	1.000	.807
Changing of business strategies without changes in business procedures (BA5)	1.000	.825
Lack of fraud risk assessment framework within the organization (BA6)	1.000	.945
Present of phishing, identity theft, card skimming, vishing, SMSishing, viruses, Deployment of keystroke loggers and Trojans, spyware and adware, website cloning and cyber stalking (BA7)	1.000	.718
Lack of sophisticated antivirus software and weak password (BA8)	1.000	.855
Irregular electricity power supply in Nigeria (BA9)	1.000	.902
Lack of fraud prevention and detection techniques and tools (BA10)	1.000	.852
Ineffective encryption backdoors (BA11)	1.000	.979
Weak litigation support in prosecution process (BA12)	1.000	.982
Poor coordination with law enforcement (BA13)	1.000	.979
Lack of rule of law (BA14)	1.000	.921
Introduction of new products without adequate control and training in place (BA15)	1.000	.787
Customers and staff unawareness to the fraud incidence (BA16)	1.000	.971
Use of the same password for different accounts (BA17)	1.000	.873
Incompetent of Anti-Crime Security Personnel (BA18)	1.000	.959
Inadequate computer knowledge and experience (BA19)	1.000	.952
Lost cards, stolen personal identification data (BA20)	1.000	.914
Pressure to meet business and personal targets influence (BA21)	1.000	.727
Spending long time on social media (BA22)	1.000	.522
Lack of oversight by senior management on deviations from existing procedure (BA23)	1.000	.538
Poor system administration and maintenances (BA24)	1.000	.563
Lack of forensic accounting professionals and absence of quality forensic analysis (BA25)	1.000	.635
Lack of dedicated technology tools for investigation (BA26)	1.000	.569
Insufficient Financial resources (BA27)	1.000	.690
Lack of competent internal auditors (BA28)	1.000	.692
In effective rule of law (BA29)	1.000	.631
In effective and lack of efficiency internet facilities (BA30)	1.000	.650
Extraction Method: Principal Component Analysis.		

Appendix 6: Communalities

	Initial	Extraction
Use of PII, Registered Phone Number, Biometrics and Data Encryption (GA5)	1.000	.425
Dedicated Forensic Technological Tools for Investigation (GA2)	1.000	.721
Bank Verification Number (Ga1)	1.000	.879
Use of Security Code, Token Cards, MasterCard Secure Code and Smart Card Authentication (GA3)	1.000	.853
Use of One-Time Password, Multi-Layer Passwords and Memorable Words (GA4)	1.000	.828
Availability of Closed Circuit Television (CCTV) Security System (GA6)	1.000	.555
Timely Access to Information by Management and Organization Learning for Fraud Prevention (GA9)	1.000	.595
Adequate Consumer Education (GA7)	1.000	.517
Effective fraud awareness Training and Seminars (GA8)	1.000	.398
Customer Screening and Employees Background Check (GA10)	1.000	.472
Automated Address Verification Service (AVS) and Automated phone call (GA14)	1.000	.448
Fraud internal control structure (GA13)	1.000	.536
Intelligence gathering mechanism(GA12)	1.000	.606
Clearly define reporting structure (GA15)	1.000	.722
Fraud risk assessment (GA11)	1.000	.876
Effective Fraud Control policy, regulation and Corporate Code of Conduct (GA16)	1.000	.551
Availability of Effective Whistle-Blower Hotline Policy (GA18)	1.000	.387
Collaboration with Government, Regulator, Law Enforcement Agency and Academia (GA17)	1.000	.404
Corporate Governance (GA6)	1.000	.631

Appendix 7: Monte Carlo PCA for Parallel Analysis Version

22/10/2017 21:53:06
Number of variables: 18
Number of subjects: 165
Number of replications: 100

Eigenvalue #	Random Eigenvalue	Standard Dev
1	1.6298	0.0734
2	1.4948	0.0503
3	1.4008	0.0462
4	1.3134	0.0354
5	1.2411	0.0313
6	1.1743	0.0277
7	1.1131	0.0284
8	1.0527	0.0279
9	0.9992	0.0261
10	0.9473	0.0265
11	0.8909	0.0295
12	0.8404	0.0281
13	0.7853	0.0291
14	0.7350	0.0272
15	0.6781	0.0275
16	0.6265	0.0290
17	0.5712	0.0326
18	0.5061	0.0364

22/10/2017 21:53:08

Monte Carlo PCA for Parallel Analysis

Appendix 8: Communalities

	Initial	Extraction
GB1	1.000	.649
GB2	1.000	.569
GB3	1.000	.532
GB4	1.000	.473
GB5	1.000	.485
GB6	1.000	.451
GB7	1.000	.440
GB8	1.000	.388
GB9	1.000	.882
GB10	1.000	.855
GB11	1.000	.622
GB12	1.000	.685
GB13	1.000	.915
GB14	1.000	.895
GB15	1.000	.871
GB16	1.000	.647
GB17	1.000	.534
GB18	1.000	.435

Extraction Method: Principal Component Analysis.

Appendix 9: Monte Carlo PCA for Parallel Analysis

```
22/10/2017   22:02:46
Number of variables:     18
Number of subjects:     165
Number of replications: 100

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Eigenvalue #     Random Eigenvalue     Standard Dev
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
      1               1.6292               .0661
      2               1.4975               .0499
      3               1.3958               .0462
      4               1.3136               .0361
      5               1.2454               .0347
      6               1.1756               .0359
      7               1.1129               .0300
      8               1.0573               .0280
      9               0.9956               .0295
     10               0.9391               .0271
     11               0.8904               .0262
     12               0.8405               .0252
     13               0.7872               .0286
     14               0.7353               .0264
     15               0.6842               .0277
     16               0.6298               .0315
     17               0.5671               .0325
     18               0.5036               .0328
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
22/10/2017   22:02:48

Monte Carlo PCA for Parallel Analysis
©2000 by Marley W. Watkins. All rights reserved.
**************************************************
```

Appendix 10: Rotation Component Matrix

Rotated Component Matrix[a]

	Component			
	1	2	3	4
GB1	.797			
GB2	.727			
GB3	.698			
GB4	.641			
GB5	.637			
GB6	.606			
GB7	.576			
GB8	.564			
GB9		.912		
GB10		.897		
GB11		.783		
GB12		.762		
GB13			.944	
GB14			.932	
GB15			.921	
GB16				.784
GB17				.661
GB18				.651

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 5 iterations.